User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7814947=
Text Part Number: 78-14947-01

Downloaded from www.Manualslib.com manuals search engine

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine
Copyright ©2002, Cisco Systems, Inc.
All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

CONTENTS

Preface xiii

- Audience xiii
- Conventions xiii
- Related Documentation xiv
- Obtaining Documentation xv
  - World Wide Web xv
  - Ordering Documentation xvi
  - Documentation Feedback xvi
- Obtaining Technical Assistance xvi
  - Cisco.com xvii
  - Technical Assistance Center xvii

CHAPTER 1 **Getting Started** 1-1

- Overview of the Wireless LAN Solution Engine 1-1
- Understanding the WLSE User Interface 1-2
  - The WLSE Dashboard 1-2
  - Device Name and IP Address Display 1-5
  - Time Display 1-5
- Logging In and Out 1-6
- Getting Started with Device Management 1-7

CHAPTER 2 **Fault Monitoring** 2-1

- Displaying Faults 2-1
  - Viewing Fault Details 2-5

Downloaded from www.Manualslib.com manuals search engine

Managing Profiles 2-7
Creating a Profile 2-8
Copying a Profile 2-8
Renaming a Profile 2-9
Editing a Profile 2-9
Deleting a Profile 2-10
Assigning a Profile to a Device 2-10
Viewing Devices 2-11
Profile Choices 2-12
Notification Settings 2-20
Setting Trap Notification 2-21
Setting Syslog Notification 2-22
Emailing Faults 2-23

CHAPTER 3 **Configuring Devices 3-1**

Using the Templates 3-1
Template Choices 3-2
Creating a Template 3-132
Copying a Template 3-133
Editing a Template 3-134
Deleting a Template 3-134
Importing a Template 3-135
Exporting a Template 3-137
Managing Configuration Jobs 3-137
Job Choices 3-138
Creating a Configuration Job 3-144
Viewing Configuration Job Status 3-144
Automating Configurations 3-151
Assigning a Startup Configuration 3-151
Creating a Startup Configuration Template 3-153

Downloaded from www.Manualslib.com manuals search engine

Assigning an Auto-Managed Configuration 3-154

CHAPTER 4 **Updating Device Firmware 4-1**

Managing Firmware Images 4-1

Viewing Images on the WLSE 4-2

Editing Image Details on the WLSE 4-3

Deleting Images from the WLSE 4-4

Importing Images 4-4

Using a Remote TFTP Server for Image Upload 4-9

Managing Firmware Jobs 4-9

Job Choices 4-10

Creating a Firmware Job 4-18

Using the Job Functions 4-18

CHAPTER 5 **Using Reports 5-1**

Using the Device Center 5-1

Viewing the Fault Summary Report 5-3

Viewing Device History 5-4

Viewing Config History 5-4

Viewing Firmware History 5-5

Displaying Wireless Client Reports 5-6

Displaying a Client Detail Report 5-6

Displaying a Client Statistics Report 5-8

Displaying a Client Historical Association Report 5-9

Displaying Current Reports 5-11

Displaying a Group Report 5-12

Displaying a Group Security Report 5-14

Displaying a Group SSID Report 5-16

Displaying a Group VLAN Report 5-18

Downloaded from www.Manualslib.com manuals search engine

Displaying a Per VLAN Client Report 5-20
Displaying a Group Policy Report 5-21
Displaying an AP Summary Report 5-24
Displaying a Detailed Report 5-26
Displaying a Current Client Association Report 5-29
Displaying an EAP Authentication Report 5-30
Displaying an AP Ethertype Protocol Filters Report 5-32
Displaying an AP IP Protocol Filters Report 5-33
Displaying an AP IP Port Filters Report 5-35
Displaying an AP Policy Report 5-36
Displaying an AP QBSS QoS Report 5-38
Displaying an AP SSID Report 5-40
Displaying an AP VLAN Report 5-42
Displaying a Per VLAN Client Report 5-43
Displaying a Switch Summary Report 5-45
Displaying an AP and Bridge Connected to Switch Report 5-46
Displaying a Router Summary Report 5-47
Displaying an AP and Bridge Connected to Router Report 5-48
Displaying a Server Summary Report 5-49
Displaying Trends 5-50
Displaying a Group Performance Report: RF Utilization 5-51
Displaying a Group Performance Report: Ethernet Utilization 5-53
Displaying a Top N Number of Associations Report 5-54
Displaying a Top N Percentage Errors 5-55
Displaying an AP and Bridge RF Transmission Statistics Report 5-56
Displaying an AP and Bridge Ethernet Transmission Statistics Report 5-58
Displaying an AP and Bridge Performance Graph 5-60
Displaying an AP and Bridge Performance: Tabular 5-61
Displaying Top N Busiest Clients 5-62
Displaying Top N Client Error Rate 5-64

Downloaded from www.Manualslib.com manuals search engine

Displaying a Server Response Time Graph 5-65
Exporting a Report 5-66
Emailing a Report 5-66
Scheduling Email Jobs 5-68
Viewing Email Job Details 5-69

CHAPTER 6 **Performing Administrative Tasks 6-1**
Using Discovery and Managing Devices 6-2
Managing Devices 6-2
Specifying Device Credentials 6-6
Managing Device Discovery 6-10
Running Inventories 6-24
Viewing Inventory and Discovery Task History 6-27
Importing Devices 6-28
Exporting Devices 6-31
Adding, Modifying and Deleting AAA Servers 6-33
Managing Groups 6-37
Overview: Groups 6-37
Creating, Editing, and Deleting Groups 6-39
Managing the Appliance 6-44
Viewing WLSE Status 6-45
Managing the Software 6-47
Overview: Security 6-55
Managing Security 6-56
Backing Up and Restoring Data 6-61
Using Diagnostics 6-64
Setting Up the Splash Screen Message 6-69
Setting the Current Time and Date on the WLSE 6-69
Specifying NTP Time Servers 6-70

Downloaded from www.Manualslib.com manuals search engine

Specifying Name Servers 6-71
Specifying an SMTP Mail Server 6-71
Using Connectivity Tools 6-72
Managing System Parameters 6-73
Administering Users 6-75
Managing Roles 6-75
Managing Users 6-77
Modifying Your Profile 6-80
Linking to a CiscoWorks2000 Server 6-81

CHAPTER 7 **Frequently Asked Questions** 7-1

CHAPTER 8 **Troubleshooting** 8-1

APPENDIX A **Naming Guidelines** A-1

APPENDIX B **Command Reference** B-1
Using the CLI B-2
CLI Conventions B-2
Command Privileges B-2
Checking Command Syntax B-2
Command History Feature B-3
Help for CLI Commands B-3
Command Summary B-4
Command Description Conventions B-9
Privilege Level 0 Commands B-10
exit B-10
ping B-10

Downloaded from www.Manualslib.com manuals search engine

show clock B-11
show domain-name B-12
show interfaces B-13
show process B-13
show version B-14
traceroute B-15
Privilege Level 15 Commands B-17
auth B-17
backup B-18
backupconfig B-19
cdp B-20
clock B-21
df B-22
erase config B-23
firewall B-24
gethostbyname B-25
hostname B-25
import B-26
install configure B-27
install list B-28
install update B-29
interface B-30
ip domain-name B-31
ip name-server B-32
listbackup B-33
mail B-34
mailcntrl clear B-35
mailcntrl list B-35
mailroute B-36
nslookup B-36

Downloaded from www.Manualslib.com manuals search engine

ntp server B-37
reload B-39
reinitdb B-40
repository B-40
repository add B-41
repository delete B-42
repository list B-43
repository server B-44
restore B-45
route B-46
services B-46
show anilog B-48
show auth-cli B-49
show auth-http B-49
show backupconfig B-50
show bootlog B-51
show cdp neighbor B-52
show cdp run B-52
show collectorlog B-53
show config B-54
show daemonslog B-55
show dmgtdlog B-56
show webaccesslog B-57
show weberrorlog B-58
show websslaccesslog B-59
show import B-59
show install logs B-60
show ipchains B-60
show hosts B-61
show maillog B-62

Downloaded from www.Manualslib.com manuals search engine

show proc B-62
show repository B-63
show route B-64
show securitylog B-64
show snmp-server B-66
show ssh-version B-66
show syslog B-67
show tech B-68
show telnetenable B-68
show tomcatlog B-69
shutdown B-70
snmp-server B-71
ssh B-71
ssh-version B-72
telnet B-72
telnetenable B-73
username B-74
Maintenance Image Commands B-75
erase config B-75
fsck B-76
reload B-76

GLOSSARY

INDEX

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Preface

This manual describes the Wireless LAN Solution Engine (WLSE) and provides instructions for using it.

Audience

This document is for system administrators responsible for managing a wireless network who are familiar with some of the concepts and terminology of Ethernet and wireless local area networking.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font

Downloaded from www.Manualslib.com manuals search engine

Item	Convention
Menu items and button names	**boldface** font
Selecting a menu item	**Option > Network Preferences**

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Note Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review the Wireless LAN Solution Engine documentation on Cisco.com for any updates.

The following additional documentation is available:

Paper Documentation

- *Installation and Configuration Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*
- *Quick Start Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*
- *Regulatory Compliance and Safety Information for the CiscoWorks 1105 Wireless LAN Solution Engine*

Downloaded from www.Manualslib.com manuals search engine

Online Documentation

- Online help—Access the online help by clicking on the Help tab.
- *Release Notes for the CiscoWorks 1105 Wireless LAN Solution Engine*
- *Integrating Cisco Applications with CiscoWorks2000 Management Connection (CMC)*
- PDF for:
  - *Installation and Configuration Guide for the CiscoWorks 1105 Warless LAN Solution Engine*
  - *Quick Start Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*
  - *Regulatory Compliance and Safety Information for the CiscoWorks 1105 Wireless LAN Solution Engine*

Note Adobe Acrobat Reader 4.0 is required.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Downloaded from www.Manualslib.com manuals search engine

Ordering Documentation

Cisco documentation is available in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Downloaded from www.Manualslib.com manuals search engine

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquires are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

Downloaded from www.Manualslib.com manuals search engine

- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

Downloaded from www.Manualslib.com manuals search engine

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Getting Started

The following topics provide an overview of the Wireless LAN Solution Engine (WLSE), information about WLSE displays, and assistance with getting started:

- Overview of the Wireless LAN Solution Engine, page 1-1
- Understanding the WLSE User Interface, page 1-2
- Logging In and Out, page 1-6
- Getting Started with Device Management, page 1-7

Overview of the Wireless LAN Solution Engine

The WLSE is a hardware and software solution for managing Cisco wireless devices. The WLSE has the following major features:

- Configuration and Firmware

  The configuration feature allows you to apply a set of configuration changes to access points and bridges. Using the firmware feature, you can upgrade the firmware on access points and bridges.

- Reporting

  Allows you to display reports for tracking device, client and security information. Reports can be emailed, printed, and exported.

- Fault and Policy Monitoring

  Provides device monitoring for fault and performance conditions, monitoring of LEAP server responses, and monitoring of policy misconfigurations.

Downloaded from www.Manualslib.com manuals search engine

The WLSE works by gathering fault, performance, and configuration information about Cisco devices that it discovers in your network. The devices must be properly configured for discovery. After devices are discovered, you decide which devices to manage with the WLSE.

Understanding the WLSE User Interface

When you log into the WLSE through the World Wide Web, the set of features (tabs and subtabs) displayed in the UI depends on the roles assigned to your user login. A user with system administrator privileges can access the features in all of the tabs and subtabs, while other users may see only a subset of features. For more information about user roles, see Managing Roles, page 6-75.

Note The WLSE UI times out after 30 minutes of inactivity and you must log in again. The timeout is not configurable.

This section describes the following aspects of the UI:

- The dashboard, including the tabs, subtabs, and buttons in the upper right corner—See The WLSE Dashboard, page 1-2.
- How device names and IP addresses are displayed in the WLSE GUI—See Device Name and IP Address Display, page 1-5.
- The way the WLSE displays timestamps—See Time Display, page 1-5.

The WLSE Dashboard

The WLSE dashboard consists of:

- Tabs and subtabs that provide access to specific functions (see Tabs and Subtabs, page 1-3).
- Buttons in the upper right corner that provide general functions (see Buttons, page 1-4).

Downloaded from www.Manualslib.com manuals search engine

Tabs and Subtabs

The dashboard contains the following tabs and subtabs:

Table 1-1 Tabs and Subtabs

Main Tab	Subtabs	For information, see...
Faults	Display faults—display device faults. Manage Profiles—use profiles to set thresholds and policies. Fault Forwarding—send fault information (traps, syslog messages, and emails)	Fault Monitoring, page 2-1.
Configure	Templates—create configuration templates. Jobs—apply configuration templates to devices. Auto update—automate initial configuration.	Configuring Devices, page 3-1.
Firmware	Images—import firmware for access points and bridges from the desktop or from Cisco.com to the WLSE. Jobs—upload firmware to devices.	Updating Device Firmware, page 4-1
Reports	Device Center—quickly view reports for a particular device. Wireless Clients—view reports about client associations with access points. Current—view, export, and email reports about each type of monitored device. Trends—view, export, and email reports about current trends for monitored devices. Scheduled email jobs—manage email jobs.	Using Reports, page 5-1.

Downloaded from www.Manualslib.com manuals search engine

Table 1-1 Tabs and Subtabs (continued)

Main Tab	Subtabs	For information, see...
Administration	Discover—run discoveries, enter device credentials, put devices under management, run immediate inventories, view task history for inventory and discovery, import and export devices, and enter AAA servers (LEAP, RADIUS, and EAP-MD5) to be monitored. Group Management—view and manage device grouping. Appliance—manage the WLSE system (view diagnostics, manage WLSE software, manage WLSE security, backup and restore data, configure the login screen, set current time, specify NTP servers and name servers, and set up routing for email jobs). System Parameters—set global parameters for inventory and polling. User Admin—manage users and user profiles. My Profile—reset your password. Connectivity Tools—use the connectivity tools (ping, traceroute, nslookup, TCP port scan, and SNMP reachability).	Performing Administrative Tasks, page 6-1.

Buttons

The four buttons in the upper right corner of the user interface have the following functions:

- Help—Displays online help for the subtab or option you are using and a table of contents and index for online help.
- About—Displays information about the WLSE version.
- Logout—Logs you out of the WLSE and displays the login screen.

Downloaded from www.Manualslib.com manuals search engine

Device Name and IP Address Display

Many WLSE displays include a field for the device name. The data displayed in this field differs depending upon the following:

- If reverse DNS lookup is enabled on the WLSE, the device name is displayed in this field if the lookup succeeds. If the lookup fails, the device IP address is displayed.
- If you do not enable reverse DNS lookup and device's sysName is set, the sysName SNMP variable is displayed. If sysName is not set, the device IP address is displayed.

In some displays there are separate fields for device name, sysName, and IP address.

To enable DNS lookup on the WLSE, select **Administration** > **Discover** > **DISCOVER** > **Discovery Options** and select Use reverse DNS lookup. For more information, see Enable Discovery Options, page 6-18.

Time Display

The WLSE uses browser (client) time in most of its displays. The format of timestamps depends on the browser you are using:

- In Internet Explorer, the timestamp usually consists of the browser time (hours:minutes:seconds) and date; for example:

  14:17:16 10/12/2002

  In some displays the timestamp is the day of the week, month and day, browser time, timezone, and year; for example:

  Sat Oct 12 11:15:01 PDT 2002

- In Netscape Navigator, the timestamp usually consists of the browser time (hours:minutes:seconds) and date; for example:

  14:17:16 10/12/2002

  In some displays the timestamp is the day of the week, time, offset from GMT/UTC, timezone, and year; for example:

  Mon Mar 25 13:29:21 GMT-0800 (Pacific Standard Time) 2002

Downloaded from www.Manualslib.com manuals search engine

It is recommended that you check the current time on the WLSE and reset it to the correct time the first time you log in. For more information about setting the current time, see Setting the Current Time and Date on the WLSE, page 6-69.

The WLSE's system time is Universal Coordinated Time (UTC), and UTC is used in certain logs, such as the Discovery Run Log. To display or reset the UTC time, use the CLI **clock** command. For more information on this command and other CLI commands, see the command reference in the *Hardware Installation and Configuration Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*—click the **PDF** button in the online help.

Logging In and Out

When user logins are set up, users are assigned one or more roles. Roles define which tabs and subtabs are visible to the user and, therefore, which features can be accessed. There are predefined roles, which can be edited but not removed; and you can create new roles. After initial setup, only the admin user can log into the WLSE, using the reserved username **admin** and the password specified during initial setup. To set up access for other users, see Managing Users, page 6-77 and Managing Roles, page 6-75.

Procedure

To log into the GUI:

Step 1 Access the WLSE through a browser by entering the WLSE's IP address, followed by **:1741** (for example: http://209.165.128:1741).

For information on supported browsers, see the *Quick Start Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*.

Step 2 Enter your username and password and click **Login**.

If you do not see features you need to use, log out and log back in as a user with those privileges. Contact the system administrator for information about the features you can access.

To log out from the WLSE, click **Logout** in the upper right corner of the window.

Downloaded from www.Manualslib.com manuals search engine

Note Login sessions automatically time out after 30 minutes of inactivity.

Getting Started with Device Management

Before you can use WLSE monitoring, configuration, firmware upgrading (or downgrading), and reporting, you must set up your devices, initiate discovery, and move devices into the managed state. To get started, follow the directions in the *Quick Start Guide for the CiscoWorks 1105 Wireless LAN Solution Engine* or use the following task list as a general guide.

Table 1-2 Basic Initial Tasks

Task	Description and References
1. Set up devices (access points, bridges, routers, switches, and AAA servers).	See Set Up Devices, page 6-12 for details.
2. Log into the WLSE using a Web browser.	Enter the WLSE's IP address, followed by:1741; for example, http://209.165.202.128:1741. Use the admin username and the password you created during initial setup of the WLSE.
3. Enter device credentials.	Device community strings for all managed devices must be entered on the WLSE. See Specifying Device Credentials, page 6-6. For access point configuration tasks, HTTP usernames and passwords must be entered on the WLSE. See Specify the HTTP Username and Password, page 6-9.
4. Initiate discovery from the WLSE or import devices from a file or from a CiscoWorks2000 server.	If you are using discovery from the WLSE, add seed devices and enable discovery. You can initiate an immediate one-time discovery or schedule discovery for a later time. See Managing Device Discovery, page 6-10.
5. Verify the discovery.	On the WLSE, verify that devices were discovered. See Viewing Inventory and Discovery Task History, page 6-27.

Downloaded from www.Manualslib.com manuals search engine

Table 1-2 Basic Initial Tasks (continued)

Task	Description and References
6. Move devices to the managed state and run inventory.	You must move devices to the managed state on the WLSE before you can use configuration, reporting, and monitoring features; or you can specify that all discovered devices be automatically managed (see Managing Devices, page 6-2). After moving devices to the managed state, you can run an immediate inventory to obtain device information needed to use such WLSE features as reports and automatic grouping (see Running Inventories, page 6-24).
7. Create other users and user roles as needed.	The WLSE has one predefined user (the system administrator with the username admin) and four predefined user roles. User roles are used to specify the WLSE functions a given user can have access to. To allow other users access to the WLSE, the system administrator must add users. The system administrator can also create roles to customize user access. See Administering Users, page 6-75.

Downloaded from www.Manualslib.com manuals search engine

Fault Monitoring

The Faults tab displays information to help you monitor your devices. All the device information shown under this tab is polled from the devices in your network.

Following are the subtabs under Faults:

Note Some of the subtabs may not be visible to some users.

- **Display Faults**—See Displaying Faults, page 2-1
- **Manage Profiles**—See Managing Profiles, page 2-7
- **Notification Settings**—See Notification Settings, page 2-20

Displaying Faults

This window displays device fault information. A fault is an abnormal condition that occurs when a system component exceeds a performance threshold or is not functioning properly. (See Specifying Fault Thresholds, page 2-15 to set threshold levels.)

A fault can also occur when a system policy is violated. (See Notification Settings, page 2-20 to set policies.)

Displayed fault information is retained by default for 30 days. To change the default, see Managing System Parameters, page 6-73.

Downloaded from www.Manualslib.com manuals search engine

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Faults** > **Display Faults**. The Fault window appears.

Step 2 Use the Filter: bar to display the faults you want to view:

Table 2-1 Display Faults Filter Bar

Field	Description
Devices	From the list, select the device type whose fault summary you want to display.
Severity	From the list, select the severity from P1, which is the highest severity level to P5, which is the lowest severity level, to display: • P1—Severity P1 faults. • P1-P2—Severity P1 and P2 faults. • P1-P3—Severity P1 through P3 faults. • P1-P4—Severity P1 through P4 faults. • P1-P5—Severity P1 through P5 faults. • All—Severity P1 through P5 faults, and faults that have been cleared.

Downloaded from www.Manualslib.com manuals search engine

Table 2-1 Display Faults Filter Bar (continued)

Field	Description
State	From the list, select a states to display: • All—Faults in all states are displayed. • Active—Faults are active (current) and have not been acknowledged. • Acknowledged—Faults that are active and have been acknowledged. • Cleared—Faults that have been cleared (no longer in an Active or Acknowledged state).
Name/IP	Enter a complete or partial device name or IP address.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Click **Apply**. The following table appears:

Note If no data is displayed in the table, there are no faults for your filtering selection to report.

Table 2-2 Display Faults Table

Column	Description
IP Address	The device IP address. Click to see various reports about the device. For information on the reports, see Using the Device Center, page 5-1.
Hostname	The device for which the fault is reported. Click to see various reports about the device. For information on the reports, see Using the Device Center, page 5-1.
Family	The product family.
Product	The product name.
Type	The device or the sub-device component.
Description	A description of the fault. Click to see fault details. See Viewing Fault Details, page 2-5.
Severity	The fault severity level.
State	The operational state of the device.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Time Display, page 1-5. Click to see fault details. See Viewing Fault Details, page 2-5.

Downloaded from www.Manualslib.com manuals search engine

Step 4 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 5 To acknowledge (change the state from Active to Acknowledged):

- A single fault, select it, then click **Acknowledge**.
- All faults, click **Select All**, then click **Acknowledge**.

Step 6 To unacknowledge (change the state from Acknowledged to Active):

- A single fault, select it, then click **Unacknowledged.**
- All faults, click **Select All,** then click **Unacknowledged**.

Related Topics

- Managing Profiles, page 2-7
- Notification Settings, page 2-20

Viewing Fault Details

The following tables are displayed in the Fault Details window.

To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Fault details for

Table 2-3 Fault Details Table

Column	Description
IP	The device IP address.
Name	The device hostname.

Downloaded from www.Manualslib.com manuals search engine

Table 2-3 Fault Details Table (continued)

Column	Description
Family	The device family.
Product	The product name.
Type	The device or the device sub-entity (which could include a logical entity, such as software or a service) in which the fault is found. **Note** If the Type is a sub-entity, additional columns appear with keys and values to help identify the precise sub-entity. These additional keys and values are MIB variables.
ifIndex	A unique number that identifies the interface.

Conditions

Table 2-4 Conditions Table

Column	Description
Name	The fault condition.
State	The state of the device.
Severity	The fault severity level.
Description	A description of the fault.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Time Display, page 1-5.

Downloaded from www.Manualslib.com manuals search engine

Fault History

Table 2-5 Fault History Table

Column	Description
State	The state of the device.
Severity	The fault severity level.
Description	A description of the fault.
Change	A description of the state change.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Time Display, page 1-5.
By	Displays the username of the person who changed the fault state. If the fault state has not been acknowledged, nothing is displayed in this column.

Managing Profiles

Every device managed by the WLSE has a profile assigned to it. A profile is made up of threshold values and policy settings.

If you have not assigned a specific profile to a device it has the system Default profile. The default profile can be edited, but it cannot be deleted.

The topics covered in this section are:

- Creating a Profile, page 2-8
- Copying a Profile, page 2-8
- Renaming a Profile, page 2-9
- Editing a Profile, page 2-9
- Deleting a Profile, page 2-10

Downloaded from www.Manualslib.com manuals search engine

- Assigning a Profile to a Device, page 2-10
- Viewing Devices, page 2-11

Creating a Profile

Use this option to create a profile.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Faults** > **Manage Profiles**. The Profiles dialog box appears.

Step 2 Enter a unique name. (See Naming Guidelines, page A-1 for details.)

Step 3 Click **Create New**. The new name appears in the Existing Profiles list.

Note The new profile is a copy of the Default profile.

Step 4 Select the name, then click **Edit**. The Editing Profile window appears. (See Editing a Profile, page 2-9.)

Copying a Profile

Use this option to copy a profile that you can use as a base for another profile.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Faults** > **Manage Profiles**. The Profiles dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Select the profile you want to copy from the Existing Profiles box, then click **Create Copy**. A dialog box appears asking you to enter a name for the copy.

Step 3 Enter a unique name. (See Naming Guidelines, page A-1 for details.)

Step 4 Click **OK**. The new name appears in the Existing Profiles list.

Step 5 Select the name, then click **Edit**. The Editing Profile window appears. (See Editing a Profile, page 2-9.)

Renaming a Profile

Use this option to rename a profile.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Faults** > **Manage Profiles.** The Profiles dialog box appears.

Step 2 Select the profile you want to rename from the Existing Profiles box, then click **Rename**. A dialog box appears asking you to enter a new name.

Step 3 Enter a unique name. (See Naming Guidelines, page A-1 for details.)

Step 4 Click **OK**. The new name appears in the Existing Profiles list.

Editing a Profile

Use this option to edit a profile.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Faults** > **Manage Profiles**. The Profiles dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Select the policy you want to edit from the Existing Policies box, then click **Edit**. The Editing Profile window appears.

Step 3 Select the policies and thresholds in the left pane that you want to assign to the profile. For a description, see Profile Choices, page 2-12.

Deleting a Profile

Use this option to delete a profile.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Faults > Manage Profiles.** The Profiles dialog box appears.

Step 2 Select the profile you want to delete from the Existing Profiles box, then click **Delete**. A window appears asking if you want to delete the profile.

Note Any devices that were assigned this deleted profile will be assigned the Default profile.

Step 3 Click **OK** to delete it.

Assigning a Profile to a Device

Use this option to assign a profile to a single device or a group of devices. Devices can only have one profile assigned to them at a time.

Note Your login determines whether you can use this option.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Faults** > **Manage Profiles.** The Profiles dialog box appears.

Step 2 Select the profile you want to assign to the devices from the Existing Profiles box, then click **Assign to Devices**. The Assigning Profiles window appears.

Step 3 If you want to search for devices, use the dialog box in the left pane above the device selector:

- **a.** From the list, select the method you want to use to search for the device: by name or by IP address.
- **b.** Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Go**. The requested device appears in the Search Results folder.

Step 4 If you know which device you want, use the device selector to select the devices. They are added to the list of Available Devices.

Step 5 From the list of Available Devices, select the device to which you want to apply the profile and click >>. The devices are moved to the Selected Devices list.

Step 6 Click **Continue**. A confirmation dialog box appears for the device assignment.

Step 7 Click **OK** to accept the device assignment or **Cancel** to cancel the device assignment.

Viewing Devices

Use this option to view the devices that have been assigned to a profile.

Note Your login determines whether you can use this option.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Faults** > **Manage Profiles.** The Profiles dialog box appears.

Step 2 Select a profile from Existing Profiles box, then click **View Devices**. A window appears listing the devices that are assigned to that profile.

Profile Choices

When you create or edit a profile, the following choices appear in the left pane of the Editing Profile window:

- **Security Policies**—See Specifying Security Policies, page 2-12
- **Thresholds**—See Specifying Fault Thresholds, page 2-15

Specifying Security Policies

This is option allows you to activate or deactivate a set of pre-defined policies for access points.

The policies you set in this window will determine how some of the faults are displayed in the **Faults** > **Display Faults** subtab.

Note Your login determines whether you can use this option.

Procedure

Step 1 In the left pane, select the variable for which you want to set a policy.

- SSID—Go to Step 2
- Firmware Version—Go to Step 5
- Broadcast SSID Disabled—Go to Step 8
- WEP Enabled—Go to Step 8
- LEAP Enabled—Go to Step 8

Downloaded from www.Manualslib.com manuals search engine

- WEP Key Length—Go to Step 10
- HTTP Disabled—Go to Step 8
- Telnet Disabled—Go to Step 8
- PSPF Enabled—Go to Step 8
- User Manager Enforced—Go to Step 8
- HTTP Authentication—Go to Step 8

Step 2 To activate the policy, do the following:

Field	Description
Verify	Select if you want to verify that SSID is enabled.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
Enter ssid	Enter the unique identifier used by client devices to associate with the access point. Any alphanumeric character up to 32 characters long.

Step 3 Click **Add** to add the SSID to the list, then go to Step 11.

Step 4 To remove an SSID from the list, select it, click **Remove**, then go to Step 11**.**

Step 5 To activate the policy, do the following:

Field	Description
Verify	Select if you want to verify that firmware version is enabled.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
Enter Firmware Version	Enter the firmware version.

Step 6 Click **Add** to add the firmware version to the list, then go to Step 11.

Downloaded from www.Manualslib.com manuals search engine

Step 7 To remove a firmware version from the list, select it, click **Remove**, then go to Step 11**.**

Step 8 Complete the following:

Field	Description
Verify	Select if you want to verify one of the following: • Broadcast SSID is disabled • WEP is enabled • LEAP is enabled • HTTP is disabled • Telnet is disabled • PSPF is enabled • User Manager Capabilities are enforced • HTTP authentication
Polling Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

Step 9 Go to Step 11.

Step 10 Complete the following:

Field	Description
Verify	Select if you want to verify the WEP key length.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
WEP Key Length	Select to indicate the bit length.

Step 11 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Downloaded from www.Manualslib.com manuals search engine

Specifying Fault Thresholds

This option allows you to set polling and exception threshold values collected from the devices you are monitoring.

The threshold values you set in this window will determine how the faults are displayed in the **Faults > Display Faults** subtab.

Note Your login determines whether you can use this option.

Threshold choices include the following options:

- **Access Point**—See Setting Access Point Fault Thresholds, page 2-15.
- **Switch**—See Setting Switch Fault Thresholds, page 2-17.
- **Router**—See Setting Router Fault Thresholds, page 2-19.
- **LEAP**—See Setting Server Response Time, page 2-19.
- **Radius**—See Setting Server Response Time, page 2-19.
- **EAP-MD5**—See Setting Server Response Time, page 2-19

Setting Access Point Fault Thresholds

Using this option, you can set up thresholds for access point faults. When the thresholds are exceeded, faults are generated and can be viewed under **Faults > Display Faults**.

Procedure

Step 1 Select any of the following to set values for:

- SNMP Reachable—Go to Step 2.
- RF Port Status—Go to Step 2.
- RF Port Utilization—Go to Step 4.
- RF Port Packet Errors—Go to Step 4.
- RF Port WEP Errors—Go to Step 4.
- RF Port FCS Errors—Go to Step 4.
- Ethernet Port Status—Go to Step 2.

Downloaded from www.Manualslib.com manuals search engine

- Ethernet Port Utilization—Go to Step 4.
- Ethernet Port Packet Errors—Go to Step 4.
- Associated Clients—Go toStep 4.
- SSID Mismatch Rate—Go toStep 4.
- Association Rate—Go to Step 4.

Step 2 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

Step 3 Continue to Step 5.

Step 4 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

Step 5 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Setting Switch Fault Thresholds

Using this option, you can set up thresholds for switch faults. When the thresholds are exceeded, faults are generated and can be viewed under **Faults > Display Faults**.

Procedure

Step 1 Select any of the following to set values for:

- SNMP Reachable —Go to Step 2.
- CPU Utilization—Go to Step 4.
- Memory Utilization—Go to Step 4.
- Port Status—Go to Step 2.
- Port Utilization—Go to Step 4.
- Module Status—Step 2.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

Step 3 Go to step Step 5.

Step 4 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

Step 5 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Downloaded from www.Manualslib.com manuals search engine

Setting Router Fault Thresholds

Using this option, you can set up the router's SNMP reachable threshold. When the threshold is exceeded, a fault is generated and can be viewed under **Faults** > **Display Faults**.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Setting Server Response Time

Using this option, you can set up a threshold for LEAP, RADIUS, and EAP-MD5 server response time. When the threshold is exceeded, a fault is generated and can be viewed under **Faults** > **Display Faults**.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the response time, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the response time, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the response time, and the number of polling cycles before the status is OK.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Notification Settings

The WLSE has the capability to send traps, syslog messages, and emails when a fault is detected.

This section has the following options:

- Setting Trap Notification
- Setting Syslog Notification
- Emailing Faults

Note Your login determines whether you can use this option.

Downloaded from www.Manualslib.com manuals search engine

Related Topics

- Displaying Faults, page 2-1
- Specifying Fault Thresholds, page 2-15
- Notification Settings, page 2-20

Setting Trap Notification

This option allows you to enable the WLSE to send north-bound exception notification to one or more SNMP trap receivers. The exception notification contains information such as device name and IP, fault number, timestamp, exception severity, and a message describing the problem.

The MIB that defines the trap and the varbinds can be found at the following URL: ftp://ftp.cisco.com/pub/mibs/v2/CISCO-DEVICE-EXCEPTION-REPORTING-MIB.my

Before You Begin

Make sure your SNMP trap receiver's trap receiving daemon is set to the correct port. The default port is set to 162.

Procedure

Step 1 Select **Faults > Notification Settings.** The Fault Notification Settings dialog box appears.

Step 2 Select the message format for the notification: Plain Text or XML.

Step 3 Complete the following:

Field	Description
Trap	Select to enable trap notification.
Port	Enter the port number if different from the default of 162.
Host	Enter the hostname/IP of the SNMP trap receiver to which you want to send SNMP trap notification.
Community	Enter the community string.

Downloaded from www.Manualslib.com manuals search engine

Step 4 If you want a different host to receive trap notification, click **add row**. There is no limit to the number you can enter.

To delete a row, click **delete,** next to the row you want to remove.

Step 5 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to save your settings.

Related Topics

- Setting Syslog Notification, page 2-22
- Emailing Faults, page 2-23

Setting Syslog Notification

This option allows you to send syslog messages to selected syslog servers. The messages contain information such as device name and IP, fault number, date and time, exception severity, and a message about what is wrong.

Before You Begin

Make sure your syslog server is turned on to be able to receive messages from the Wireless LAN Solution Engine. Also make sure that the receiving process is configured to receive messages from remote hosts (for example, start syslogd with -r option on some UNIX versions).

Procedure

Step 1 Select **Faults > Notification Settings.** The Fault Notification Settings dialog box appears.

Step 2 Select the message format for the notification: Plain Text or XML.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Complete the following:

Field	Description
Syslog	Select to send syslog messages to designated syslog servers.
Enter Syslog host names	Enter the hostname/IP for the syslog servers. Names must be separated by a space, a comma, a semicolon, or a new line.

Step 4 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to save your settings.

Related Topics

- Setting Trap Notification, page 2-21
- Emailing Faults, page 2-23

Emailing Faults

The emailed exception notification contains the following information:

Attribute	Description
FaultId	A unique identifier for the fault.
DeviceId	A unique identifier used by the WLSE for the device with the fault.
DeviceIp	The IP address of the device with the fault.
DeviceName	The name of the device with the fault.
MOId	The identifier used by the WLSE for the subcomponent of the device with the fault.
AlarmState	The state of the Alarm (Active or Cleared).
Description	A description of the last updated to the fault.
Severity	The severity of the fault.

Downloaded from www.Manualslib.com manuals search engine

You have the option of sending the email notification as plain text or in an XML format.

- An example of a message using plain text will appear as follows:

```
FaultId 19
DeviceId 106
DeviceIp 172.20.29.118
DeviceName sj-W-10-AP-118
MOId {MOID[c=1013,d=106,i=379]}
AlarmState Active
Description SSID policy violation
Severity P1
```

- An example of the same message sent in an XML format will appear as follows:

```
<Msg><FaultId>19</FaultId><DeviceId>106</DeviceId><DeviceIP>172.
20.29.118</DeviceIP><DeviceName>sj-W-10-AP-118<DeviceName><MOId>
{MOID[c=1013,d=106,i=379]}</MOId><AlarmState>Active</AlarmState>
<Description>SSID policy violation
</Description><Severity>P1</Severity></Msg>
```

Procedure

Step 1 Select **Faults > Notification Settings.** The Fault Notification Settings dialog box appears.

Step 2 Select the message format for the notification: Plain Text or XML.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Complete the following:

Field	Description
Email	Select to enable email notification of exception information.
Enter email addresses	Enter the email addresses of users you want to receive exception notification. Addresses must be separated by a space, a comma, a semicolon, or a new line.
Priority	From the list, select the priority of the exceptions you want to email.

Tip If email notification is not working, you may need to configure the mailroute by selecting **Administration > Appliance > Configure Mailroute**.

Step 4 If you want a different group of users to receive different priority level exceptions, click **add row** to add another set of email addresses. There is no limit to the number of email addresses you can enter.

Step 5 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to save your settings.

Related Topics

- Setting Trap Notification, page 2-21
- Setting Syslog Notification, page 2-22

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Configuring Devices

The Configure tab allows you to view, create, copy, edit, and delete configuration templates and apply them to large numbers of devices at a time.It also allows you to schedule a configuration job and to check on the job's status.

Following are the subtabs under Configure:

Note Some of the subtabs may not be visible to some users.

- **Templates**—See Using the Templates, page 3-1.
- **Jobs**—See Managing Configuration Jobs, page 3-137.
- **Auto Update**—See Automating Configurations, page 3-151.

Using the Templates

This is window allows you to create, modify, and delete configuration templates.

The topics covered in this section are:

- Creating a Template, page 3-132
- Copying a Template, page 3-133
- Editing a Template, page 3-134
- Deleting a Template, page 3-134

Downloaded from www.Manualslib.com manuals search engine

- Importing a Template, page 3-135
- Exporting a Template, page 3-137

Related Topic

Managing Configuration Jobs, page 3-137

Template Choices

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

When you create or edit a configuration template, the following choices appear in the left pane of the Templates window:

1. **Template Name**—See Naming the Template, page 3-3.
2. **Template Categories**

Note Any or all of the template categories can be completed in any order.

   - **Express Template**—See Using Express Template, page 3-3.
   - **Association**—See Setting Up Association, page 3-8.
   - **Ethernet**—See Configuring the Ethernet Port, page 3-49.
   - **11b Radio**—See Configuring the 11b Radio, page 3-56.
   - **11a Radio**—See Configuring the 11a Radio, page 3-73.
   - **Security**—See Defining the Security Settings, page 3-92.
   - **Services**—See Configuring Services, page 3-102.
   - **Events**—See Configuring Events, page 3-124.
   - **Custom Values**—See Configuring Custom Values, page 3-130.
3. **Preview**—See Previewing the Template, page 3-131.
4. **Finish**—See Finishing the Template, page 3-132.

Downloaded from www.Manualslib.com manuals search engine

Naming the Template

This option enables to you to name the template.

Procedure

Note Clicking **Clear** removes all the entries you have made.

Step 1 Select **Template Name**. The Template Name dialog box appears:

Field	Description
Name	Enter a name for the template. See Naming Guidelines, page A-1.
Description	Enter a description of the purpose of the template. See Naming Guidelines, page A-1

Step 2 Select a template category. (For additional information, see Template Categories, page 3-2.)

Using Express Template

Use this option if you need to set up an access point quickly with a simple configuration. This will allow you to enter all the access point's essential settings for basic operation.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Express Template**. The Express dialog box displays in the right pane:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-1 Express Template Settings

Field	Description
Reboot Device	From the list, select Yes if you want to allow device reboots.
SysName	Enter a system name. The system name appears in the titles of the management system pages and in the access point's Association Table page. This is not an essential setting, but it helps identify the access point on your network.
SysLocation	Enter the system's location. This is not an essential setting, but it helps identify the access point on your network.
SysContact	Enter a contact name. This is not an essential setting but it helps identify the person responsible for the access point on your network.

Downloaded from www.Manualslib.com manuals search engine

Table 3-1 Express Template Settings (continued)

Field	Description
Configuration Server Protocol	Set this entry to match the network's method of IP address assignment. From the list, select one of the following options: • None-Static IP—Use this if your network does not have an automatic system for IP address assignment. • BOOTP—Use this if your network uses Bootstrap Protocol, in which IP addresses are hard-coded based on MAC addresses. • DHCP—Use this if your network uses Dynamic Host Configuration Protocol, in which IP addresses are "leased" for predetermined periods of time.
Default Subnet Mask	Enter an IP subnet mask to identify the subnetwork so the IP address can be recognized on the LAN. If DHCP or BOOTP is not enabled, this field is the subnet mask. If DHCP or BOOTP is enabled, this field provides the subnet mask only if no server responds to the access point's DHCP or BOOTP request.
Default Gateway	Enter the IP address of your default Internet gateway. The entry 255.255.255.255 indicates no gateway.

Downloaded from www.Manualslib.com manuals search engine

Table 3-1 Express Template Settings (continued)

Field	Description
Radio Service Set ID (SSID)	Enter any alphanumeric, case-sensitive string, from 2 to 32 characters long. The SSID is a unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity and provides access to VLANs by wireless client devices. Several access points on a network or subnetwork can share an SSID.

Downloaded from www.Manualslib.com manuals search engine

Table 3-1 Express Template Settings (continued)

Field	Description
Role in Network	From the list, select one of the following: • Access Point—Use this setting if the access point is connected to the wired LAN. • Repeater—Use this setting for access points not connected to the wired LAN. • Survey Client—Use this setting when performing a site survey for a repeater access point. When you select this setting, clients are not allowed to associate and the bridge's STP function is disabled. • Root Bridge—Use this setting to set a bridge as the root bridge. (One bridge in each group of bridges must be set as the root bridge). The root bridge cannot associate with another root bridge. • Non-Root Bridge w/ Client—Use this setting for non-root bridges that accept associations from client devices and for bridges acting as repeaters. A non-root bridge will only associate to another bridge (root or non-root). • Non-Root Bridge w/o Client—Use this setting for non-root bridges that should not accept associations from client devices. A non-root bridge (without clients) can connect to a wired LAN and only associates to another bridge (root or non-root).

Downloaded from www.Manualslib.com manuals search engine

Table 3-1 Express Template Settings (continued)

Field	Description
Ensure Compatibility with Cisco	From the list, select one of the following: • Enable—Use this setting to automatically configure the device to be compatible with other Cisco devices on your wireless LAN. • Disable—Use this setting to not automatically configure the device to be compatible with other Cisco devices on your wireless LAN.
Ensure Compatibility with 2MB/sec Clients	From the list, select one of the following: • Enable— Use this setting to operate at a maximum speed of two megabits per second. • Disable—Use this setting if you do not want devices to operate at a maximum speed of two megabits per second.

Step 2 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Setting Up Association

Use this option to set up spanning tree protocol (STP) on bridges and to set up filtering to control the flow of data through the access point.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Association**. The menu expands and the Association dialog box displays in the right pane.

Step 2 Select one of the following from the Association menu:

- Spanning Tree—See Defining Spanning Tree Protocol, page 3-9.
- Address Filters—See Defining Address Filters, page 3-12.
- Ethertype Filters—See Defining Ethertype Filters, page 3-14.
- IP Protocol Filters—See Defining IP Protocol Filters, page 3-18.
- IP Port Filters—See Defining IP Port Filters, page 3-23.
- Policy Groups—See Configuring Policy Groups, page 3-28.
- VLANs—See Configuring VLANs, page 3-31.
- Quality of Service—See Configuring Quality of Service, page 3-36.
- Service Sets—See Configuring Service Sets, page 3-38.
- Advanced—See Defining Advanced Associations, page 3-42.
- Port Assignments—See Configuring Port Assignments, page 3-47.
- DSCP to CoS—See Configuring DSCP to CoS, page 3-48.

Defining Spanning Tree Protocol

This option is used for only bridges.

Procedure

Step 1 Select **Association > Spanning Tree**. The Association: Spanning Tree Protocol dialog box appears.

Step 2 Click **see details** for information on which bridges this configuration is valid.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-2 Spanning Tree Protocol Settings

Field	Description
Spanning Tree Protocol (STP)	From the list, select one of the following: • Enable—Use this setting to enable STP on the bridge. • Disable—If you do not want STP enabled the bridge.
Always Unblock Ethernet when STP is disabled	From the list, select one of the following: • Yes—Use this setting to maintain a bridge link when STP is disabled • No—Use this setting to not maintain a bridge link when STP is disabled. Click **see details** to see which versions this setting is valid for.
Root Configuration	
Priority (0-65535)	Enter a number to influence which bridge is designated the root bridge in the spanning tree. When bridges have the same priority setting, STP uses the MAC addresses as a tiebreaker. The bridge with the lowest priority setting is likely to be designated the root bridge in the tree.

Downloaded from www.Manualslib.com manuals search engine

Table 3-2 Spanning Tree Protocol Settings (continued)

Field	Description
Max Age (6-40 Seconds)	Enter the number of seconds to define how long the bridge waits before deciding the network has changed and the spanning tree needs to be rebuilt. For example, with Max Age set to 20, the bridge attempts to rebuild the spanning tree if it does not receive a hello BDPU from the root bridge in the spanning tree within 20 seconds.
Hello Time (1-10 Seconds)	Enter the number of seconds to define how often the root bridge in the spanning tree sends out a hello BPDU telling the other bridges that the network topology has not changed and that the spanning tree should remain the same.
Forward Delay (4-30 Seconds)	Enter the number of seconds to define how long the bridge's ports should stay in the listening and learning transition states if there is a change in the spanning tree.
Port Configuration	
Path Cost (1-65535)	Enter a number to indicates the relative efficiency of a port's network link. A port with a high path cost is less likely to become a bridge's root port.
Priority (0-255)	Enter a number to influence whether STP designates a port as a bridge's root port. A port with a low priority setting is more likely to become a bridge's root port.
Enable	From the list, select one of the following for each port configured: • Enable—Use this setting to indicate whether the port participates in STP. (This determines whether the port blocks or forwards traffic.) • Disable—Use this setting to indicate that the port does not participate in STP.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining Address Filters

Using this option, you can:

- Create a MAC address filter
- Remove a MAC address filter

Procedure

Step 1 Select **Association > Address Filters**. The Association: Address Filters dialog box appears.

Step 2 To add a new MAC address filter complete the following fields:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Lookup MAC address on Authentication Server if not in an Existing Filter List?	Click one of the following: • Yes—Use this setting to allow looking up a MAC address on the authentication server. • No—Use this setting to disallow looking up a MAC address.
Is MAC Authentication alone sufficient for a client to be fully authenticated?	From the list, select one of the following: • Yes—Use this setting to specify that client devices that associate to the access point using 802.11 open authentication, first attempt MAC authentication. • No—Use this setting to specify that MAC authentication alone is not sufficient. Click **see details** to see which versions this setting is valid for.
New Destination MAC Address	Enter a destination MAC address by entering the address in one of the following ways: • With colons separating the character pairs (00:40:96:12:34:56, for example) • Without any intervening characters (004096123456, for example)
Allowed	Click to pass traffic to the MAC address.
Disallowed	Click to discard traffic to the MAC address.

Step 3 Click **Add** to add the MAC address to the Current MAC Address Filters list.

Step 4 To remove a MAC Address, select it from the Current MAC Address Filters list, then click **Remove**.

Downloaded from www.Manualslib.com manuals search engine

Step 5 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining Ethertype Filters

Procedure

Step 1 Select **Association > Ethertype Filters.** The Association: Ethertype Filters dialog box appears.

Step 2 Using this option:

- Create new filters—See Creating New Ethertype Filters, page 3-14.
- Delete the Filters—See Deleting Ethertype Filters, page 3-16.

Using this option you can also:

- Create Special Cases—See Creating Special Cases, page 3-16.
- Delete Special Cases—See Deleting Special Cases, page 3-18.

Creating New Ethertype Filters

Procedure

Step 1 To create and enable protocol filters for the access point's Ethernet port, enter the following:

Note Refer to the following URL for a list of Ethertype protocols: http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350axb.htm#85314

Downloaded from www.Manualslib.com manuals search engine

Table 3-3 Creating New Ethertype Filters Settings

Field	Description
Add New Ethertype Filter	
Set ID	Enter an identification number for the filter set.
Set Name	Enter a descriptive filter set name. See Naming Guidelines, page A-1.
Default Disposition	From the list, select one of the following: • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.
Default Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.

Step 2 Click **Add.** The new name is added to the Ethertype Filters list.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Deleting Ethertype Filters

Procedure

Step 1 To delete protocol filters for the access point's Ethernet port, select the set name from the Current Ethertype Filters list, then click **Delete**.

Step 2 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Creating Special Cases

Procedure

Step 1 Select the default filter for which you want to define a special case.

Step 2 Enter the following:

Table 3-4 Ethertype Filter Special Cases Settings

Field	Description
Special Cases	
Ethertype	Enter the Ethertype filter name.
Disposition	From the list, select one of the following: • Default—Use the disposition you set for the Ethertype filter. • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.

Downloaded from www.Manualslib.com manuals search engine

Table 3-4 Ethertype Filter Special Cases Settings (continued)

Field	Description
Priority	From the list, select one of the following: • Default—This setting is the same as best effort, which applies to normal LAN traffic. • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Excellent Effort—Use this setting for a network's most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10 ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.
Alert	From the list, select one of the following: • yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point. • no—Use this setting to not send an alert to the event log.

Step 3 Click **Add.** The new name is added to the list box.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting Special Cases

Procedure

Step 1 To delete special cases for the access point's Ethernet port, select the Ethertype name from the list box, then click **Delete**.

Step 2 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining IP Protocol Filters

Procedure

Step 1 Select **Association > IP Protocol Filters.** The Association: IP Protocol Filters dialog box appears.

Step 2 With this option you can:

- Create new filters—See Creating New IP Protocol Filters, page 3-19.
- Delete the filters—See Deleting IP Protocol Filters, page 3-20.

Downloaded from www.Manualslib.com manuals search engine

Using this option you can also:

- Create Special Cases —See Creating Special Cases, page 3-21.
- Delete Special Cases—See Deleting Special Cases, page 3-23.

Creating New IP Protocol Filters

Procedure

Step 1 To create and enable IP protocol filters, enter the following:

Note Refer to the following URL for a list of IP protocols: http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350axb.htm#85314

Field	Description
Add New Protocol Filter	
Set ID	Enter an identification number for the filter set.
Set Name	Enter a descriptive filter set name. See Naming Guidelines, page A-1.
Default Disposition	From the list, select one of the following: • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.
Default Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Click **Add.** The new name is added to the Current Protocol Filters list.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting IP Protocol Filters

Procedure

Step 1 To delete an IP protocol filter, select the name from the Current Protocol Filters list, then click **Delete**.

Step 2 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Creating Special Cases

Procedure

Step 1 Select the default filter for which you want to define a special case.

Step 2 Enter the following:

Table 3-5 IP Protocol Filters Special Cases Settings

Field	Description
Special Cases	
Protocol	Enter the IP protocol name.
Disposition	From the list, select one of the following: • Default—Use the disposition you set for the protocol filter. • Forward—Use this setting to forward traffic. • Block—Use this setting to block traffic.

Downloaded from www.Manualslib.com manuals search engine

Table 3-5 IP Protocol Filters Special Cases Settings (continued)

Field	Description
Priority	From the list, select one of the following: • Default—This setting is the same as best effort, which applies to normal LAN traffic. • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Excellent Effort—Use this setting for a network's most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10 ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.
Alert	From the list, select one of the following: • yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point. • no—Use this setting to not send an alert to the event log.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Click **Add.** The new name is added to the list box.

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting Special Cases

Procedure

Step 1 To delete special cases, select the protocol name from the list box, then click **Delete**.

Step 2 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining IP Port Filters

Procedure

Step 1 Select **Association > IP Port Filters.** The Association: IP Port Filters dialog box appears.

Step 2 With this option you can:

- Create new filters—See Creating New Port Filters, page 3-24.
- Delete the filters—See Deleting Port Filters, page 3-25.

Downloaded from www.Manualslib.com manuals search engine

Using this option you can also:

- Create Special Cases —See Creating Special Cases, page 3-26.
- Delete Special Cases—See Deleting Special Cases, page 3-28.

Creating New Port Filters

Procedure

Step 1 To create and enable port filters, enter the following:

Note Refer to the following URL for a list of IP port protocols: http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350axb.htm#85314

Field	Description
Add New Protocol Filter	
Set ID	Enter an identification number for the filter set.
Set Name	Enter a descriptive filter set name. See Naming Guidelines, page A-1.
Default Disposition	From the list, select one of the following: • Forward—Use this setting to forward traffic. • Block—Use this setting to block traffic.
Default Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.

Step 2 Click **Add.** The new name is added to the Current Port Filters list.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting Port Filters

Procedure

Step 1 To delete a protocol filter, select the name from the Current Port Filters list, then click **Delete**.

Step 2 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Creating Special Cases

Procedure

Step 1 Select the default filter for which you want to define a special case.

Step 2 Enter the following:

Table 3-6 IP Port Filters Special Cases Settings

Field	Description
Special Cases	
Port	Enter the IP Port filter name.
Disposition	From the list, select one of the following: • Default—Use the disposition you set for the port filter. • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.

Downloaded from www.Manualslib.com manuals search engine

Table 3-6 IP Port Filters Special Cases Settings (continued)

Field	Description
Priority	From the list, select one of the following: • Default—This setting is the same as best effort, which applies to normal LAN traffic. • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Excellent Effort—Use this setting for a network's most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10 ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the buffer before they are discarded.
Alert	From the list, select one of the following: • yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point. • no—Use this setting to not send an alert to the event log.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting Special Cases

Procedure

Step 1 To delete special cases, select the port name from the list box, then click **Delete**.

Step 2 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Policy Groups

Policy groups are used to configure access parameters to a logical group of stations in a consistent manner from a single place. For example, protocol filters can be applied to frames for a selected group of stations.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Association > Policy Group**. The Association: Policy Group dialog box appears.

Step 2 Click **see details** to see which versions this option is valid for.

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Step 3 Using this option you can:

- Add and delete a policy group—See Adding or Deleting a New Policy Group, page 3-29.
- Delete an exiting Policy Group From a Device—See Deleting an Existing Policy Group from a Device, page 3-30.

Adding or Deleting a New Policy Group

Step 1 To add a new policy group, enter the following:

Field	Description
GroupID	Enter an identification number for the policy group.
Group Name	Enter a name for the policy group.
Ethertype	
Receive	Enter the ID of a defined Ethertype filter, or select one of the filters you created using **Association > Ethertype Filters**.
Transmit	Enter the ID of a defined Ethertype filter, or select one of the filters you created using **Association > Ethertype Filters**.
IP Protocol	

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Receive	Enter the ID of a defined IP protocol filter, or select one of the filters you created using **Association > IP Protocol Filters**.
Transmit	Enter the ID of a defined IP protocol filter, or select one of the filters you created using **Association > IP Protocol Filters**.
IP Port	
Receive	Enter the ID of a defined IP port filter, or select one of the filters you created using **Association > IP Port Filters**.
Transmit	Enter the ID of a defined IP port filter, or select one of the filters you created using **Association > IP Port Filters**.

Step 2 Click **Add** to add the group to the Policy Groups to Add list.

Step 3 To delete a group from the Policy Groups to Add list, select the group name, then click **Delete.**

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting an Existing Policy Group from a Device

Step 1 Enter the group identification number in the **Group ID** text box, then click **Add** to add it to the Policy Groups to Delete list.

Downloaded from www.Manualslib.com manuals search engine

Step 2 To delete an identification number from the Policy Groups to Delete list, select it, then click **Delete**.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring VLANs

Access points and bridges in a VLAN network, which are running specific software versions, can provide a wireless VLAN trunk link between two wired segments of the network.

Using this option, you can configure VLANs on the access point.

Procedure

Step 1 Select **Association** > **VLANs**. The Association: VLAN dialog box appears.

Step 2 Click **see details** to see which versions this option is valid for.

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Enter the following information:

Field	Description
VLAN (802.1Q) Tagging	From the list, select one of the following: • Enabled—Use this setting to allow IEEE 802.1Q protocol tagging on VLAN packets. The IEEE 802.1Q protocol is used to interconnect multiple switches and routers, and for defining VLAN topologies. • Disabled—Use this setting to not allow tagging.
Native VLAN ID	Enter identification number of the access point's native VLAN. **Note** This setting must agree with the native VLAN ID setting on the switch.
Single VLAN ID which allows unencrypted packets	Enter an identification number to allow unencrypted packets. An entry with a value of 0 (zero) requires the use of encryption.
Optionally allow Point-to-point Packet Encryption	From the list, select one of the following: • Yes—Use this setting to allow point-to-point encryption. • No—Use this setting to not allow point-to-point encryption.

Step 4 Using this option you can:

- Add a new VLAN—See Adding a New VLAN, page 3-33.
- Delete an exiting VLAN from a Device—See Deleting an Existing VLAN, page 3-36.

Downloaded from www.Manualslib.com manuals search engine

Adding a New VLAN

Step 1 To add a new VLAN, enter the following:

Table 3-7 Adding a New VLAN Settings

Field	Description
VLAN ID	Enter the identification number of the VLAN. **Note** This setting must match the setting on the switch.
VLAN Name	Enter the a unique name for the VLAN configured on the access point.
VLAN Enable	From the list, select one of the following: • Enabled—Use this setting to enable the VLAN. • Disabled—Use this setting to disable the VLAN.
Default Priority	From the list, select one of the following: • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Default—Use this setting for normal LAN traffic. • Excellent Effort—Use this setting for the network's most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Default Policy Group	Enter the default policy group number, or select one you created using **Association > Policy Groups**.

Downloaded from www.Manualslib.com manuals search engine

Table 3-7 Adding a New VLAN Settings (continued)

Field	Description
Enhanced MIC verify WEP	From the list, select one of the following: • None—Use this setting if you do not want Message Integrity Check (MIC) enabled. • MMH—Use this setting if you want MIC enabled to protect WEP keys. **Note** When you enable MIC, only MIC-capable client devices can communicate with the access point.
Temp Key Integrity Protocol	From the list, select one of the following: • None—Use this setting if you do not want to enable the temporal key integrity protocol (TKIP, or WEP key hashing.) • Cisco—Use this setting to enable TKIP. **Note** When TKIP is enabled, all WEP-enabled client devices associated to the access point must support WEP key hashing, or they will not be able to communicate with the access point.
WEP Key Rotation Interval	Use this setting to enable or disable broadcast key rotation. • To enable it, enter the rotation interval in seconds. If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. **Note** When you enable broadcast key rotation, only wireless client devices using LEAP or EAP-TLS authentication can use the access point. Client devices using static WEP (with open, shared key, or EAP-MD5) cannot use the access point when you enable broadcast key rotation. • To disable it, enter 0 (zero).

Downloaded from www.Manualslib.com manuals search engine

Table 3-7 Adding a New VLAN Settings (continued)

Field	Description
Alert	From the list, select one of the following: • Yes—Use this setting if you are not adding an encrypted VLAN. • No—Use this setting if you are adding an encrypted VLAN.
WEP Keys 1 through 4	Enter the encryption keys used: 40 bit or 128 bit hexadecimal digits.
Size	For each WEP key, select one of the following: Not set, 40 bit, or 128 bit.

Step 2 Click **Add** to add the VLAN to the VLANs to Add list.

Downloaded from www.Manualslib.com manuals search engine

Step 3 To delete a group from the VLANs to Add list, select the name, then click **Delete.**

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting an Existing VLAN

Procedure

Step 1 Enter the VLAN identification number in the **VLAN ID** text box, then click **Add** to add it to the VLANs to Delete list.

Step 2 To delete an identification number from the VLANs to Delete list, select it, then click **Delete**.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Quality of Service

This option is used to configure the access point's Quality of Service feature.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Association** > **Quality of Service**. The Association: Quality of Service dialog box appears.

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Step 2 Click **see details** to see which versions this option is valid for.

Step 3 Enter the following information:

Table 3-8 Quality of Service Settings

Field	Description
Generate QBBS Element	From the list, select one of the following: • Yes—Use this setting to enable support for basic 802.11 Quality of Service. • No—Use this setting to disable support for basic 802.11 Quality of Service.
User Symbol Extensions	From the list, select one of the following: • Yes—Use this setting enables support for Symbol Voice over IP (VoIP) phones. • No—Use this setting to disable support for Symbol VoIP phones.
Send IGMP General Query	From the list, select one of the following: • Yes—Use this setting to allow the access point to send an IGMP General Query to all associated stations when they complete all required high-level authentication. • No—Use this setting to not allow the access point to send an IGMP General Query.

Downloaded from www.Manualslib.com manuals search engine

Table 3-8 Quality of Service Settings (continued)

Field	Description
Background	From the **CWmin** and **CWmax** lists, select the minimum and maximum contention window values for each traffic category.
(spare)	
Best Effort (default)	
Excellent Effort	
Controlled Load	
Interactive Video	
Interactive Voice	
Network Control	

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Service Sets

This option allows you to define service sets.

Procedure

Step 1 Select **Association** > **Service Sets**. The Association: Service Sets dialog box appears.

Step 2 Click **see details** to see which versions this option is valid for.

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Using this option you can:

- Add a new Service Set—See Adding a New Service Set, page 3-39.
- Delete an exiting Service Set from a device—See Deleting an Existing Service Set, page 3-42.

Adding a New Service Set

Procedure

Step 1 To add a new Service set, enter the following:

Table 3-9 New Service Set Settings

Field	Description
Service Set ID (1-24)	Enter an identification number for your SSID.
Service Set Name	Enter a unique name for the wireless VLAN.
Maximum Number of Associations	Enter a number to limit the maximum number of wireless clients per SSID.
Proxy Mobile IP Enabled	From the list, select one of the following: • Yes—This setting allows proxy mobile IP use by all stations associated to this access point. • No—This setting does not allow proxy mobile IP use.
Default VLAN ID	Enter the identification number for a defined VLAN, or select one of the VLAN IDs you created using **Association >VLANs**.
Default Policy Group	Enter the identification number of a defined policy group, or select one of the policy groups you created using **Association > Policy Groups**.
Accept Authentication Type	

Downloaded from www.Manualslib.com manuals search engine

Table 3-9 New Service Set Settings (continued)

Field	Description
Open	From the list, select one of the following: • Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting. • No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.
Shared	From the list, select one of the following: • Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting. • No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.
Network-EAP	From the list, select one of the following: • Yes—Allows EAP-enabled client devices to authenticate through the access point. • No—Does not allow EAP-enabled client devices to authenticate through the access point.
Require EAP	
Open	From the list, select one of the following: • Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use open and EAP authentication.

Downloaded from www.Manualslib.com manuals search engine

Table 3-9 New Service Set Settings (continued)

Field	Description
Shared	From the list, select one of the following: • Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use shared and EAP authentication.
Default Unicast Address Filter	
Open Shared Network-EAP	From the list, select one of the following: • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server. Select Disallowed for each authentication type that also uses MAC-based authentication.

Step 2 Click **Add** to add the Service Set to the Service Sets to Add list.

Step 3 To delete a group from the list, select the name, then click **Delete.**

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Deleting an Existing Service Set

Procedure

Step 1 Enter the Service Set number in the **Service Set ID** text box, then click **Add** to add it to the Service Sets to Delete list.

Step 2 To delete an identification number from the list, select it, then click **Delete**.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining Advanced Associations

Use this option to control the total number of devices an access point can list in the Association Table and the amount of time the access point continues to track each device class when a device is inactive.

Procedure

Step 1 Select **Association** > **Advanced**. The Association: Advanced dialog box appears.

Step 2 To define advanced associations, enter the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Downloaded from www.Manualslib.com manuals search engine

Table 3-10 Advanced Association Settings

Field	Description
Alert Severity Level	From the list select one of the following: • systemFatal—Indicates an event that prevents operation of the port or device. • protocolFatal—Indicates an event that prevents operation of the port or device • portFatal—Indicates an event that prevents operation of the port or device • systemAlert—Indicates that you need to take action to correct the condition. • protocolAlert—Indicates that you need to take action to correct the condition. • portAlert—Indicates that you need to take action to correct the condition. • externalAlert—Indicates that you need to take action to correct the condition.

Downloaded from www.Manualslib.com manuals search engine

Table 3-10 Advanced Association Settings (continued)

Field	Description
	• systemWarning—Indicates that an error or failure may have occurred. • protocolWarning—Indicates that an error or failure may have occurred. • portWarning—Indicates that an error or failure may have occurred. • externalWarning—Indicates that an error or failure may have occurred. • systemInfo—Notification that some sort of event has occurred. • protocolInfo—Notification that some sort of event has ocurred. • portInfo—Notification that some sort of event has ocurred. • externalInfo—Notification that some sort of event has ocurred.
Max Bytes Stored Per Alert Packet	Enter the maximum number of bytes the access point stores for each Station Alert packet when packet tracing is enabled. If you use 0, the access point does not store bytes for Station Alert packets; it only logs the event.
Max Fwd Table Entries	From the list, select one of the following to designate the maximum number of devices that can appear in the Association Table: 1024, 2048, 4096, 8192, 16384, 32768, 65536.

Downloaded from www.Manualslib.com manuals search engine

Table 3-10 Advanced Association Settings (continued)

Field	Description
Enable Extended Stats in MIB	From the list, select one of the following: • Enable—Use this setting to enable the storage of detailed statistics in the device's memory. • Disable—Use this setting to disable the storage of detailed statistics in the device's memory. When you disable extended statistics you conserve memory, and the device can include more devices in the Association Table.
Enable PSPF	From the list, select one of the following: • Enable—Use this setting to enable Publicly Secure Packet Forwarding, which ensures that client devices cannot communicate with other client devices on the wireless network. This feature is useful for public wireless networks like those installed in airports or on college campuses. • Disable—Use this setting to disable Publicly Secure Packet Forwarding. Click **see details** to see which versions this setting is valid for.

Downloaded from www.Manualslib.com manuals search engine

Table 3-10 Advanced Association Settings (continued)

Field	Description
Unknown Class Timeout	Enter the number of seconds the access point continues to track an inactive device depending on its class. A setting of zero tells the access point to track a device indefinitely no matter how long it is inactive. A setting of 300 equals 5 minutes; 1800 equals 30 minutes; 28800 equals 8 hours.
Multicast Addresses Timeout	
Infrastructure Hosts Timeout	
Client Stations Timeout	
Repeaters Timeout	
Access Points Timeout	
Across Bridge Hosts Timeout	
Non-Root Bridges Timeout	
Root Bridges Timeout	

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Configuring Port Assignments

When you assign specific ports, your network topology remains constant even when devices reboot.

Procedure

Step 1 Select **Association** > **Port Assignments**. The Association: Port Assignments dialog box appears.

Step 2 To define port assignments, enter the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-11 Port Assignments Settings

Field	Description
ifIndex	Lists the port's designator in the Standard MIB-II (RFC1213-MIB.my) interface index.
dot1dBasePort	Lists the port's designator in the Bridge MIB (RFC1493; BRIDGE-MIB.my) interface index.
AID	Lists the port's 802.11 radio drivers association identifier.
Station	Enter the MAC address of the device to which you want to assign the port.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Configuring DSCP to CoS

This option is use to statically map Differentiated Services Code-Point (DSCP) values to corresponding Class of Service (CoS) values.

Procedure

Step 1 Select **Association > DSCP to CoS**. The Association: DSCP to CoS Conversion dialog box appears.

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Step 2 Click **see details** to see which versions this option is valid for.

Step 3 For each DSCP, enter the CoS conversion. Select one of the following:

- No Change
- Background
- Spare
- Best Effort
- Excellent Effort
- Controlled Load
- Interactive Video
- Interactive Voice
- Network Control

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Configuring the Ethernet Port

Use this option to configure the device's Ethernet port.

Procedure

Step 1 Select **Ethernet**. The menu expands and the Ethernet dialog box displays in the right pane.

Step 2 Select one of the following from the Ethernet menu:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Identification—See Identifying the Ethernet Port, page 3-49.
- Filters—See Setting Up Ethernet Filters, page 3-50.
- Hardware—See Setting Up Hardware, page 3-52.
- Advanced—See Defining the Ethernet Advanced Settings, page 3-53.

Identifying the Ethernet Port

Use this option to define basic identity information for the Ethernet port.

Procedure

Step 1 Select **Ethernet > Identification**. The Ethernet: Identification dialog box displays in the right pane.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Enter the following information to identify the port:

Table 3-12 Ethernet Port Settings

Field	Description
Primary Port?	From the list, select one of the following: • Ethernet—Sets the Ethernet port for all access points other than AP1200's as the primary port. • Ethernet AP 1200—Sets the Ethernet port for AP1200 access points as the primary port. • Radio 11b—Sets the 11b radio port as the primary port. • Radio 11a—Sets the 11a radio port as the primary port.
Adopt Primary Port Identity?	From the list, select one of the following: • yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port. • no—This uses different MAC and IP addresses for the Ethernet port.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Setting Up Ethernet Filters

Use this option to define filters for the Ethernet port, the IP Protocol, and the IP Port.

Downloaded from www.Manualslib.com manuals search engine

Note Changing this setting may cause the access point to reboot.

Procedure

Step 1 Select **Ethernet** > **Filters**. The Ethernet: Filters dialog box displays in the right pane.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-13 Ethernet Filters Settings

Field	Description
Ethertype	
Receive	Enter the ID of a defined Ethertype filter, or select one of the filters you created using **Association** > **Ethertype Filters**.
Transmit	Enter the ID of a defined Ethertype filter, or select one of the filters you created using **Association** > **Ethertype Filters**.
IP Protocol	
Receive	Enter the ID of a defined IP protocol filter, or select one of the filters you created using **Association** > **IP Protocol Filters**.
Transmit	Enter the ID of a defined IP protocol filter, or select one of the filters you created using **Association** > **IP Protocol Filters**.
IP Port	
Receive	Enter the ID of a defined IP port filter, or select one of the filters you created using **Association** > **IP Port Filters**.
Transmit	Enter the ID of a defined IP port filter, or select one of the filters you created using **Association** > **IP Port Filters**.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Setting Up Hardware

This option allows you to select the hardware settings used by the access point's Ethernet port.

Procedure

Step 1 Select **Ethernet > Hardware**. The Ethernet: Hardware dialog box displays in the right pane.

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Step 2 Click **see details** to see which versions this option is valid for.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Complete the following:

Table 3-14 Ethernet Hardware Settings

Field	Description
Loss of Backbone Connectivity # of Secs (1-1000)	Enter the number of seconds the system must detect loss of backbone connectivity (i.e. loss of Ethernet link and no active trunk available on any of the radios) before taking the specified by Loss of Backbone Connectivity Action.
Loss of Backbone Connectivity Action	From the list, select one of the following: • No action • Switch to repeater mode • Shut the radio off • Restrict to SSID
Loss of Backbone Connectivity SSID	Enter an SSID index required if the Loss of Backbone Connectivity Action is set to Restrict to SSID, or select the SSID from the list.

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining the Ethernet Advanced Settings

Use this option to define the settings and operational status of the Ethernet port.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Ethernet > Advanced**. The Ethernet: Advanced dialog box displays in the right pane.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-15 Ethernet Advanced Settings

Field	Description
Status	From the list, select one of the following: • up— Enables the Ethernet port for normal operation. • down—Disables the device's Ethernet port.
Packet Forwarding	From the list, select one of the following: • enabled—Allows normal operation. • disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.
Default Multicast Address Filter	From the list, select one of the following: • allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under **Association > Address Filters**. • disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under **Association > Address Filters**.

Downloaded from www.Manualslib.com manuals search engine

Table 3-15 Ethernet Advanced Settings (continued)

Field	Description
Maximum Multicast Packets/Second	Use this setting to control the number of multicast packets that can pass through the Ethernet port each second. If you enter 0, the access point passes an unlimited number of multicast packets. If you enter a number other than 0, the device passes only that number of multicast packets per second.
Default Unicast Address Filter	From the list, select one of the following: • allowed—The access point forwards all traffic except packets sent to MAC addresses that have been set as disallowed under **Association > Address Filters**. • disallowed—The access point discards all traffic except packets sent to the MAC addresses that have been set as allowed under **Association > Address Filters**.
Always Unblock Ethernet when STP is disabled	From the list, select one of the following: From the list, select one of the following: • Yes—Use this setting to maintain a bridge link when STP is disabled • No—Use this setting to not maintain a bridge link when STP is disabled. Click **see details** to see which versions this setting is valid for.
Optimize Ethernet for	From the list, select one of the following: • Performance—Allows faster packet forwarding. • Statistics Collection—Allows better statistics collection. Click **see details** to see which versions this setting is valid for.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring the 11b Radio

Use this option to configure the device's 11b radio.

Procedure

Step 1 Select **11b Radio**. The menu expands and the Radio dialog box displays in the right pane.

Step 2 Select one of the following from the Radio menu:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Identification—See Identifying the 11b Radio Port, page 3-56.
- Filters—See Setting Up 11b Radio Filters, page 3-59.
- Hardware—See Defining the 11b Radio Hardware Settings, page 3-60.
- Advanced—See Defining the 11b Radio Advanced Settings, page 3-66.
- Searched Channels—See Defining the 11b Radio Searched Channels Settings, page 3-71.

Identifying the 11b Radio Port

Use this option to define basic identity information for the port.

Downloaded from www.Manualslib.com manuals search engine

Note Changing this setting may cause the access point to reboot.

Procedure

Step 1 Select **11b Radio** > **Identification**. The 11b Radio: Identification dialog box displays in the right pane.

Step 2 Enter the following information to identify the port:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Downloaded from www.Manualslib.com manuals search engine

Table 3-16 11b Radio Identification Settings

Field	Description
Primary Port?	From the list, select one of the following: **Note** If the primary port was set using **Ethernet > Identification**, the selected value is displayed. • Ethernet—Sets the Ethernet port for all access points other than AP1200's as the primary port. • Ethernet AP 1200—Sets the Ethernet port for AP1200 access points as the primary port. • Radio 11b—Sets the 11b radio port as the primary port. • Radio 11a—Sets the 11a radio port as the primary port.
Adopt Primary Port Identity?	From the list, select one of the following: • yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port. • no—This uses different MAC and IP addresses for the Ethernet port.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Setting Up 11b Radio Filters

Note Changing this setting may cause the access point to reboot.

Procedure

Step 1 Select **11b Radio > Filters**. The 11b Radio Filters dialog box displays in the right pane.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-17 11b Radio Filters Settings

Field	Description
Ethertype	
Receive	Enter the ID of a defined Ethertype filter, or select one of the filters you created using **Association > Ethertype Filters**.
Transmit	Enter the ID of a defined Ethertype filter, or select one of the filters you created using **Association > Ethertype Filters**.
IP Protocol	
Receive	Enter the ID of a defined IP protocol filter, or select one of the filters you created using **Association > IP Protocol Filters**.
Transmit	Enter the ID of a defined IP protocol filter, or select one of the filters you created using **Association > IP Protocol Filters**.

Downloaded from www.Manualslib.com manuals search engine

Table 3-17 11b Radio Filters Settings (continued)

Field	Description
IP Port	
Receive	Enter the ID of a defined IP port protocol filter, or select one of the filters you created using **Association > IP Port Filters**.
Transmit	Enter the ID of a defined IP port protocol filter, or select one of the filters you created using **Association > IP Port Filters**.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining the 11b Radio Hardware Settings

Procedure

Step 1 Select **11b Radio > Hardware**. The 11b Radio: Hardware dialog box displays in the right pane.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-18 11b Radio Hardware Settings

Field	Description
Service SetID (SSID)	Enter a unique identifier client devices use to associate with the access point. It can be any alphanumeric, case-sensitive string, from 2 to 32 characters long. Several access points on a network or sub-network can share an SSID.
Allow “Broadcast” SSID to Associate	From the list, select one of the following: • yes—Allows devices that do not specify an SSID (devices that are “broadcasting” in search of an access point to associate with) to associate with the access point. • no—Does not allow devices that do not specify an SSID (devices that are “broadcasting” in search of an access point to associate with) to associate with the access point. With no selected, the SSID used by the client device must match exactly the access point’s SSID.

Downloaded from www.Manualslib.com manuals search engine

Table 3-18 11b Radio Hardware Settings (continued)

Field	Description
Enable “World Mode” multi-domain operation?	From the list, select one of the following: • yes—Allows the access point to add channel carrier set information to its beacon. Client devices with world-mode enabled receive the carrier set information and adjust their settings automatically. • no—Does not allow the access point to add channel carrier set information to its beacon.
Data Rates (Mb/sec)	
1.0	From the list, select one of the following for each of the four rates in megabits per second: • basic—Allows transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to basic. • yes—Allows transmission at this rate for unicast packets only. • no—Does not allow transmission at this rate.
2.0	
5.5	
11.0	
Transmit Power	From the list, select one of the following milliwatt settings: 1, 5, 20, 30, 50, 100. To reduce interference or to conserve power, select a lower power setting. Click **see details** to see which versions this setting is valid for.

Downloaded from www.Manualslib.com manuals search engine

Table 3-18 11b Radio Hardware Settings (continued)

Field	Description
Fragmentation Threshold (256-2338)	Enter a setting to determine the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
RTS Threshold (0-2339)	Enter a setting to determine the packet size at which the access point issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the access point and not each other.
Maximum RTS Retries (1-128)	Enter the maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio.
Max. Data Retires (1-128)	Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.
Beacon Period (Kusec)	Enter the amount of time between beacons in kilomicroseconds. (One kilomicrosecond equals 1,024 microseconds.)

Downloaded from www.Manualslib.com manuals search engine

Table 3-18 11b Radio Hardware Settings (continued)

Field	Description
Data Beacon Rate (DTIM)	Enter the amount of time, always a multiple of the beacon period, to determine how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them. If the beacon period is set at 100, its default setting, and the data beacon rate is set at 2, its default setting, then the access point sends a beacon containing a DTIM every 200 kilomicrosecond.
Default Radio Channel	From the list, select the radio channel you want for a default. Each channel covers 22 MHz. The factory setting for Cisco wireless LAN systems is Radio Channel 6 transmitting at 2437 MHz.
Search for less-congested Radio Channel?	From the list, select one of the following: • yes—Allows the access point to scan for the radio channel that is least busy and selects that channel for use. • no—Will not allow the access point to scan for a radio channel that is least busy.

Downloaded from www.Manualslib.com manuals search engine

Table 3-18 11b Radio Hardware Settings (continued)

Field	Description
Receive Antenna	From the list, select one of the following:
Transmit Antenna	• Right—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's right connector. (When you look at the access point's back panel, the right antenna is on the right.) Use this setting for both receive and transmit. • Left—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector. (When you look at the access point's back panel, the left antenna is on the left.) Use this setting for both receive and transmit. • Diversity—Use this setting if your access point has two fixed (non-removable) antennas; it tells the access point to use the antenna that receives the best signal. Use this setting for both receive and transmit.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining the 11b Radio Advanced Settings

Use this option to define the settings and operational status of the Ethernet port.

Procedure

Step 1 Select **11b Radio** > **Advanced**. The 11b Radio: Advanced dialog box displays in the right pane.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Downloaded from www.Manualslib.com manuals search engine

Table 3-19 11b Radio Advance Settings

Field	Description
Status	From the list, select one of the following: • up— Enables the Radio port for normal operation. • down—Disables the device's Radio port.
Packet Forwarding	From the list, select one of the following: • enabled—Allows normal operation. • disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.
Default Multicast Address Filter	From the list, select one of the following: • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under **Association > Address Filters**. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under **Association > Address Filters**.
Maximum Multicast Packets/Second	Use this setting to control the number of multicast packets that can pass through the Ethernet port each second. If you enter 0, the access point passes an unlimited number of multicast packets. If you enter a number other than 0, the device passes only that number of multicast packets per second.

Downloaded from www.Manualslib.com manuals search engine

Table 3-19 11b Radio Advance Settings (continued)

Field	Description
Maximum Number of Associations	Enter the maximum number of wireless networking devices that are allowed to associate to the access point. If you enter 0 it means that the maximum possible number of associations is allowed. Click **see details** to see which versions this setting is valid for.
Use Aironet Extensions	From the list, select one of the following: • yes—Enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • no—Does no enable the features listed above.
Classify Workgroup Bridges as network infrastructure	From the list, select one of the following: • yes—Use this setting to limit the number of workgroup bridges that can associate to the access point to 20 or less. • no—Use this setting to allow more than 20 workgroup bridges to associate to the access point. Click **see details** to see which versions this setting is valid for.
User Symbol Extensions	From the list, select one of the following: • yes—Use this setting to enable the following features: load balancing, message integrity check (MIC), temporal key integrity protocol (TKIP). • no—Use this setting to disable use of Cisco Aironet 802.11 extensions. Click **see details** to see which versions this setting is valid for.

Downloaded from www.Manualslib.com manuals search engine

Table 3-19 11b Radio Advance Settings (continued)

Field	Description
Ethernet encapsulation transform	From the list, select one of the following: • 802.1H—Provides optimum performance for Cisco Aironet wireless products. • RFC1042—Ensures interoperability with non-Cisco Aironet wireless equipment.
Enhanced MIC verification for WEP	From the list, select one of the following: • None—Does not enable MIC. • NMH—Enables MIC (Message Integrity Check), a security feature that protects your WEP keys by preventing attacks on encrypted packets called bit-flip attacks. Click **see details** to see for which versions this setting is valid.
Temporal Key Integrity Protocol	From the list, select the following: • None—Does not enable WEP key hashing. • Cisco—Enables WEP key hashing that defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key. Click **see details** to see which versions this setting is valid for.

Downloaded from www.Manualslib.com manuals search engine

Table 3-19 11b Radio Advance Settings (continued)

Field	Description
Broadcast WEP Key rotation interval (sec)	Enter a rotation interval in seconds. • If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. • If you enter 0, you disable broadcast WEP key rotation. Click **see details** to see which versions this setting is valid for.
Default Unicast Address Filter	
Open Shared Network-EAP	From the list, select one of the following: • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server. Select Disallowed for each authentication type that also uses MAC-based authentication.
Specified Access Point 1 Specified Access Point 2 Specified Access Point 3 Specified Access Point 4	If this access point is a repeater, enter the MAC address of one or more root-unit access points with which you want this access point to associate. With MAC addresses in these fields, the repeater access point always tries to associate with the specified access points instead of with other less-efficient access points.

Downloaded from www.Manualslib.com manuals search engine

Table 3-19 11b Radio Advance Settings (continued)

Field	Description
Radio Modulation	From the list, select one of the following: • Standard—This setting is the modulation type specified in IEEE 802.11, the wireless standard published by the Institute of Electrical and Electronics Engineers (IEEE) Standards Association. • MOK—This modulation was used before the IEEE finished the high-speed 802.11 standard and may still be in use in older wireless networks.
Radio Preamble	From the list, select one of the following: • Long—Ensures compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A). • Short—Cisco Aironet's Wireless LAN Adapter supports short preambles; it improves throughput performance.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining the 11b Radio Searched Channels Settings

Use this option to limit the channels that the access point scans when Search for less-congested radio channel is enabled.

Downloaded from www.Manualslib.com manuals search engine

The access point uses this setting to scan for the radio channel that is least busy and selects that channel for use.

Procedure

Step 1 Select **11b Radio > Searched Channels**. The 11b Radio: Searched Channels dialog box displays in the right pane.

Step 2 Click **see details** to see which versions this option is valid for.

Step 3 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-20 11b Radio Searched Channels Settings

Field	Description
Channel Number	Lists the available channels by number.
Frequency (mHz)	Lists the channel frequency.
Search?	From the list, select one of the following: • Yes—Use this option to include the channel in the scan for less-congested channels. • No—Use this option to exclude the channel in the scan for less-congested channels

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Configuring the 11a Radio

Use this option to configure the device's 11a radio.

Procedure

Step 1 Select **11a Radio**. The menu expands and the 11a Radio dialog box displays in the right pane.

Step 2 Click **see details** to see which versions this option is valid for.

Step 3 Select one of the following from the Radio menu:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Identification—See Identifying the 11a Radio Port, page 3-73.
- Filters—See Setting Up 11a Radio Filters, page 3-75.
- Hardware—See Defining the 11a Radio Hardware Settings, page 3-76.
- Advanced—See Defining the 11a Radio Advanced Settings, page 3-81.
- Searched Channels—See Defining the 11a Radio Searched Channels Settings, page 3-88.
- Data Encryption—See Defining the 11a Radio Data Encryption Settings, page 3-89.

Identifying the 11a Radio Port

Use this option to define basic identity information for the Ethernet port.

Note Changing this setting may cause the access point to reboot.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **11a Radio** > **Identification**. The 11a Radio: Identification dialog box displays in the right pane.

Step 2 Click **see details** to see which versions this option is valid for.

Step 3 Enter the following information to identify the port:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-21 11a Radio Identification Settings

Field	Description
Primary Port?	From the list, select one of the following: **Note** If the primary port was set using **Ethernet** > **Identification**, the selected value is displayed. • Ethernet—Sets the Ethernet port for all access points other than AP1200's as the primary port. • Ethernet AP 1200—Sets the Ethernet port for AP1200 access points as the primary port. • Radio 11b—Sets the 11b radio port as the primary port. • Radio 11a—Sets the 11a radio port as the primary port.
Adopt Primary Port Identity?	From the list, select one of the following: • yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port. • no—This uses different MAC and IP addresses for the Ethernet port.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Setting Up 11a Radio Filters

Note Changing this setting may cause the access point to reboot.

Procedure

Step 1 Select **11a Radio > Filters**. The 11a Radio Filters dialog box displays in the right pane.

Step 2 Click **see details** to see which versions this option is valid for.

Step 3 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-22 11a Radio Filters Settings

Field	Description
Ethertype	
Receive	Enter the ID of a defined Ethertype filter, or select one of the filters you created using **Association > Ethertype Filters**.
Transmit	Enter the ID of a defined Ethertype filter, or select one of the filters you created using **Association > Ethertype Filters**.

Downloaded from www.Manualslib.com manuals search engine

Table 3-22 11a Radio Filters Settings (continued)

Field	Description
IP Protocol	
Receive	Enter the ID of a defined IP protocol filter, or select one of the filters you created using **Association > IP Protocol Filters**.
Transmit	Enter the ID of a defined IP protocol filter, or select one of the filters you created using **Association > IP Protocol Filters**.
IP Port	
Receive	Enter the ID of a defined IP port protocol filter, or select one of the filters you created using **Association > IP Port Filters**.
Transmit	Enter the ID of a defined IP port protocol filter, or select one of the filters you created using **Association > IP Port Filters**.

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining the 11a Radio Hardware Settings

Procedure

Step 1 Select **11a Radio > Hardware**. The 11a Radio: Hardware dialog box displays in the right pane.

Step 2 Click **see details** to see which versions this option is valid for.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-23 11a Radio Hardware Settings

Field	Description
Service SetID (SSID)	Enter a unique identifier client devices use to associate with the access point. It can be any alphanumeric, case-sensitive string, from 2 to 32 characters long. Several access points on a network or sub-network can share an SSID.
Allow “Broadcast” SSID to Associate	From the list, select one of the following: • yes—Allows devices that do not specify an SSID (devices that are “broadcasting” in search of an access point to associate with) to associate with the access point. • no—Does not allow devices that do not specify an SSID (devices that are “broadcasting” in search of an access point to associate with) to associate with the access point. With no selected, the SSID used by the client device must match exactly the access point’s SSID.

Downloaded from www.Manualslib.com manuals search engine

Table 3-23 11a Radio Hardware Settings (continued)

Field	Description
Data Rates (Mb/sec)	
6.0	From the list, select one of the following for each of the four rates in megabits per second: • basic—Allows transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to basic. • yes—Allows transmission at this rate for unicast packets only. • no—Does not allow transmission at this rate.
9.0	
12.0	
18.0	
24.0	
36.0	
48.0	
54.0	
Transmit Power	From the list, select one of the following milliwatt settings: 5, 10, 20, 40. To reduce interference or to conserve power, select a lower power setting. Click **see details** to see which versions this setting is valid for.
Fragmentation Threshold (256-2338)	Enter a setting to determine the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
RTS Threshold (0-2339)	Enter a setting to determine the packet size at which the access point issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the access point and not each other.

Downloaded from www.Manualslib.com manuals search engine

Table 3-23 11a Radio Hardware Settings (continued)

Field	Description
Maximum RTS Retries (1-128)	Enter the maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio.
Max. Data Retires (1-128)	Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.
Beacon Period (Kusec)	Enter the amount of time between beacons in kilomicroseconds. (One kilomicrosecond equals 1,024 microseconds.)
Data Beacon Rate (DTIM)	Enter the amount of time, always a multiple of the beacon period, to determine how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them. If the beacon period is set at 100, its default setting, and the data beacon rate is set at 2, its default setting, then the access point sends a beacon containing a DTIM every 200 Kmsecs. (One Kmsec equals 1,024 microseconds.)
Default Radio Channel	From the list, select the radio channel you want for a default.
Search for less-congested Radio Channel?	From the list, select one of the following: • yes—Allows the access point to scan for the radio channel that is least busy and selects that channel for use. • no—Will not allow the access point to scan for a radio channel that is least busy.

Downloaded from www.Manualslib.com manuals search engine

Table 3-23 11a Radio Hardware Settings (continued)

Field	Description
Receive Antenna	From the list, select one of the following:
Transmit Antenna	• Right—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's right connector. (When you look at the access point's back panel, the right antenna is on the right.) Use this setting for both receive and transmit. • Left—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector. (When you look at the access point's back panel, the left antenna is on the left.) Use this setting for both receive and transmit. • Diversity—Use this setting if your access point has two fixed (non-removable) antennas; it tells the access point to use the antenna that receives the best signal. Use this setting for both receive and transmit.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining the 11a Radio Advanced Settings

Use this option to define the settings and operational status of the Ethernet port.

Procedure

Step 1 Select **11a Radio** > **Advanced**. The 11a Radio: Advanced dialog box displays in the right pane.

Step 2 Click **see details** to see which versions this option is valid for.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-24 11a Radio Advanced Settings

Field	Description
Status	From the list, select one of the following: • up—Enables the Radio port for normal operation. • down—Disables the device's Radio port.
Packet Forwarding	From the list, select one of the following: • enabled—Allows normal operation. • disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.
Default Multicast Address Filter	From the list, select one of the following: • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under **Association > Address Filters**. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under **Association > Address Filters**.
Maximum Multicast Packets/Second	Use this setting to control the number of multicast packets that can pass through the Ethernet port each second. If you enter 0, the access point passes an unlimited number of multicast packets. If you enter a number other than 0, the device passes only that number of multicast packets per second.

Downloaded from www.Manualslib.com manuals search engine

Table 3-24 11a Radio Advanced Settings (continued)

Field	Description
Radio Cell Role	From the list, enter one of the following: • Client/Non-Root—use this setting for diagnostics or site surveys, such as when you need to test and access point by having it communicate with another access point or bridge without accepting associations from client devices. • Repeater/Non-Root—Use this setting for access points that are not connected to a wired LAN and which transfer data between another access point or repeater. • Access Point/Root—Use this setting if the access point is connected to a wired LAN.
Maximum Number of Associations	Enter the maximum number of wireless networking devices that are allowed to associate to the access point. If you enter 0 it means that the maximum possible number of associations is allowed. Click **see details** to see which versions this setting is valid for.
Use Aironet Extensions	From the list, select one of the following: • yes—Enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • no—Does no enable the features listed above.

Downloaded from www.Manualslib.com manuals search engine

Table 3-24 11a Radio Advanced Settings (continued)

Field	Description
Classify Workgroup Bridges as network infrastructure	From the list, select one of the following: • yes—Use this setting to limit the number of workgroup bridges that can associate to the access point to 20 or less. • no—Use this setting to allow more than 20 workgroup bridges to associate to the access point.
Ethernet encapsulation transform	From the list, select one of the following: • 802.1H—Provides optimum performance for Cisco Aironet wireless products. • RFC1042—Ensures interoperability with non-Cisco Aironet wireless equipment.
Enhanced MIC verification for WEP	From the list, select one of the following: • None—Does not enable MIC. • NMH—Enables MIC (Message Integrity Check), a security feature that protects your WEP keys by preventing attacks on encrypted packets called bit-flip attacks.
Temporal Key Integrity Protocol	From the list, select the following: • None—Does not enable WEP key hashing. • Cisco—Enables WEP key hashing that defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key.

Downloaded from www.Manualslib.com manuals search engine

Table 3-24 11a Radio Advanced Settings (continued)

Field	Description
Broadcast WEP Key rotation interval (sec)	Enter a rotation interval in seconds. • If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. • If you enter 0, you disable broadcast WEP key rotation.
Accept Authentication Type	
Open	From the list, select one of the following: • Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting. • No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.
Shared	From the list, select one of the following: • Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting. • No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.

Downloaded from www.Manualslib.com manuals search engine

Table 3-24 11a Radio Advanced Settings (continued)

Field	Description
Network-EAP	From the list, select one of the following: • Yes—Allows EAP-enabled client devices to authenticate through the access point. • No—Does not allow EAP-enabled client devices to authenticate through the access point.
Require EAP	
Open	From the list, select one of the following: • Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use open and EAP authentication.
Shared	From the list, select one of the following: • Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use shared and EAP authentication.

Downloaded from www.Manualslib.com manuals search engine

Table 3-24 11a Radio Advanced Settings (continued)

Field	Description
Default Unicast Address Filter	
Open Shared Network-EAP	From the list, select one of the following: • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server. Select Disallowed for each authentication type that also uses MAC-based authentication.
Specified Access Point 1 Specified Access Point 2 Specified Access Point 3 Specified Access Point 4	If this access point is a repeater, enter the MAC address of one or more root-unit access points with which you want this access point to associate. With MAC addresses in these fields, the repeater access point always tries to associate with the specified access points instead of with other less-efficient access points.

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Defining the 11a Radio Searched Channels Settings

Use this option to limit the channels that the access point scans when Search for less-congested radio channel is enabled.

The access point uses this setting to scan for the radio channel that is least busy and selects that channel for use.

Procedure

Step 1 Select **11a Radio > Searched Channels**. The 11a Radio: Searched Channels dialog box displays in the right pane.

Step 2 Click **see details** to see which versions this option is valid for.

Step 3 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-25 11a Radio Searched Channels Settings

Field	Description
Channel Number	Lists the available channels by number.
Frequency (mHz)	Lists the channel frequency.
Search?	From the list, select one of the following: • Yes—Use this option to include the channel in the scan for less-congested channels. • No—Use this option to exclude the channel in the scan for less-congested channels

Downloaded from www.Manualslib.com manuals search engine

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining the 11a Radio Data Encryption Settings

Use this option to limit the channels that the access point scans when Search for less-congested radio channel is enabled.

The access point uses this setting to scan for the radio channel that is least busy and selects that channel for use.

Procedure

Step 1 Select **11a Radio > Data Encryption**. The 11a Radio: Data Encryption dialog box displays in the right pane.

Step 2 Click **see details** to see which versions this option is valid for.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Complete the following:

Table 3-26 11a Radio Data Encryption Settings

Field	Description
Data Encryption by Stations	From the list, select the encryption type: • No Encryption—Requires clients to communicate with the Access Point without any data encryption. This setting is not recommended. • Optional—Allows clients to communicate with the Access Point either with or without data encryption. Typically, this option is used when you have client devices that cannot make a WEP connection, such as non-Cisco clients in a 128-bit WEP environment. • Full Encryption—Requires clients to use data encryption when communicating with the Access Point. Clients not using data encryption are allowed to communicate. This option is recommended if you want to maximize the security of your Wireless LAN.
Authentication Type	
Open	From the list, select one of the following: • Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting. • No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.

Downloaded from www.Manualslib.com manuals search engine

Table 3-26 11a Radio Data Encryption Settings (continued)

Field	Description
Shared Key	From the list, select one of the following: • Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting. • No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.
Require EAP	
Open	From the list, select one of the following: • Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use open and EAP authentication.
Shared	From the list, select one of the following: • Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use shared and EAP authentication.
Encryption Keys 1 through 4	
Transmit Key	Click to indicate this is the key you want to use to transmit packets. Only one key can be selected at a time.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)Another template category to configure more options. (See Template Categories, page 3-2.)

Defining the Security Settings

Use this option to configure the device's security settings.

Procedure

Step 1 Select **Security**. The menu expands and the Security dialog box displays in the right pane.

Step 2 Select one of the following from the Security menu:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Local Admin Access—See Setting Local Admin Access, page 3-92.
- Local AP/Client Security—See Setting Local AP/Client Security, page 3-94.
- Server-Based Security—See Setting Server-Based Security, page 3-97.

Setting Local Admin Access

Use this option to enable or disable local admin access.

Procedure

Step 1 Select **Security > Local Admin Access**. The Security: Local Admin Access dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-27 Local Admin Access Settings

Field	Description
Local Admin Authentication	Select **Enable** to enable local admin authentication, or **Disable** to disable it.
Allow read-only browsing without login	Select **Yes** to allow it, or **No** to disallow it.

Step 3 Using this option you can:

- Add Users—See Adding Users, page 3-93.
- Delete Users—See Deleting Users, page 3-94.

Adding Users

Procedure

Step 1 To add a new user, enter the following:

Field	Description
User ID	Enter an identification number for the user. **Tip** If you want to set the same user name on all access points and do not know which user ID's may already be in use, enter a very high value (2000).
User name	Enter the name for the user.
User password	Enter a password for the user.
Capabilities	Select the capabilities you want to allow the user.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Click **Add** to add the users to the Users to Add list.

Step 3 To delete a user from the list, select the name, then click **Delete.**

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting Users

Click **see detail** to see which versions this option is valid for.

Procedure

Step 1 Enter the user's identification number in the **User ID** text box, then click **Add** to add it to the Users to Delete list.

Step 2 To delete an identification number from the list, select it, then click **Delete**.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Setting Local AP/Client Security

Use this option to set up the local access point and client security.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Security > Local AP/Client Security.** The Security: Local AP/Client Security dialog box appears:

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-28 Local AP /Client Security Settings

Field	Description
Data Encryption by Stations	From the list, select the encryption type: • No Encryption—Requires clients to communicate with the Access Point without any data encryption. This setting is not recommended. • Optional—Allows clients to communicate with the Access Point either with or without data encryption. Typically, this option is used when you have client devices that cannot make a WEP connection, such as non-Cisco clients in a 128-bit WEP environment. • Full Encryption—Requires clients to use data encryption when communicating with the Access Point. Clients not using data encryption are allowed to communicate. This option is recommended if you want to maximize the security of your Wireless LAN.
Authentication Type	
Open	From the list, select one of the following: • Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting. • No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.

Downloaded from www.Manualslib.com manuals search engine

Table 3-28 Local AP /Client Security Settings (continued)

Field	Description
Shared Key	From the list, select one of the following: • Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting. • No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.
Network-EAP	From the list, select one of the following: • Yes—Allows EAP-enabled client devices to authenticate through the access point. • No—Does not allow EAP-enabled client devices to authenticate through the access point.
Require EAP	
Open	From the list, select one of the following: • Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use open and EAP authentication.
Shared	From the list, select one of the following: • Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use shared and EAP authentication.
Encryption Keys 1 through 4	

Downloaded from www.Manualslib.com manuals search engine

Table 3-28 Local AP /Client Security Settings (continued)

Field	Description
Transmit Key	Click to indicate this is the key you want to use to transmit packets. Only one key can be selected at a time.
Encryption Key	Enter the type of encryption key used: • For 40-bit WEP keys, enter as 10 hexadecimal digits (0-9, a-f, or A-F). • For 128-bit WEP keys, enter as 26 hexadecimal digits (0-9, a-f, or A-F).
Key Size	From the list, select one of the following: • Not set • 40 bit • 128 bit

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Setting Server-Based Security

Use this option to set up server-based security.

Note Changing this setting may cause the access point to reboot.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Security** > **Server-Based Security.** The Security: Server-Based dialog box appears:

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Downloaded from www.Manualslib.com manuals search engine

Table 3-29 Server-Based Security Settings

Field	Description
802.1X Protocol Version (For EAP Authentication)	**Note** This setting may cause the device to reboot. From the list, select one of the following: • Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting. • Draft 8—Select this option if LEAP-enabled client devices that associate with this access point use radio firmware versions 4.13, 4.16, or 4.23, or if workgroup bridges associating with this access point use firmware version 8.58 or earlier. • Draft 10—Select this option if client devices that associate with this access point or bridge use Microsoft Windows XP EAP authentication, if LEAP-enabled client devices that associate with this bridge use radio firmware version 4.25 or later, or if workgroup bridges associating with this access point use firmware version 8.65 or later. Click ***** (asterisk) for information on which version this setting is valid
Primary Server Reattempt Period (Min)	Enter the amount of time a before another attempt is made if the server is not responding. Click ***** (asterisk) for information on which version this setting is valid.
Server Name/IP	Enter the name or IP address of the server.

Downloaded from www.Manualslib.com manuals search engine

Table 3-29 Server-Based Security Settings (continued)

Field	Description
Server Type	Enter the type of server. Click * (asterisk) for information on which version this setting is valid
Port	Enter the port number your server uses for authentication.
Shared Secret	Enter the shared secret used by your server. It must match the shared secret on the RADIUS server.
Retran Int (sec)	Enter the number of seconds the access point should wait before retransmitting. Click * (asterisk) for information on which version this setting is valid.
Time Out (sec's)	Enter the number of seconds the access point should wait before authentication fails. If the server does not respond within this time, the access point tries to contact the next defined authentication server.
EAP Auth	From the list, select one of the following: • Yes—Use this server for EAP authentication. In this type of authentication, the access point relays authentication messages between the server and the authenticating client device. • No—Do not use this server for EAP authentication. Click * (asterisk) for information on which version this setting is valid.

Downloaded from www.Manualslib.com manuals search engine

Table 3-29 Server-Based Security Settings (continued)

Field	Description
MAC Auth	From the list, select one of the following: • Yes—Use this server for MAC-based authentication. This allows only client devices with specified MAC addresses to associate and pass data through the access point. Client devices with MAC addresses not in a list of allowed MAC addresses are not allowed to associate with the access point. • No—Do not use this server for MAC-based authentication. Click * (asterisk) for information on which version this setting is valid.
User Auth	From the list, select one of the following: • Yes—Use this setting to allow user authentication. • No—Use this setting to disallow user authentication. Click * (asterisk) for information on which version this setting is valid.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Configuring Services

Use this option to configure various system features and support services on the device.

Procedure

Step 1 Select **Services**. The menu expands and the Services dialog box displays in the right pane.

Step 2 Select one of the following from the Services menu:

- Start-Up—See Configuring Start-Up Settings, page 3-103.
- Console/Telnet—See Configuring Console/Telnet Settings, page 3-107.
- Hot Standby—See Configuring Hot Standby Settings, page 3-109.
- Routing—See Configuring Routing Settings, page 3-111.
- CDP—See Configuring CDP Settings, page 3-112.
- DNS—See Configuring DNS Settings, page 3-113.
- FTP—See Configuring FTP Settings, page 3-114.
- HTTP—See Configuring HTTP Settings, page 3-116.
- SNMP—See Configuring SNMP Settings, page 3-117.
- SNTP—See Configuring SNTP Settings, page 3-118.
- Accounting—See Configuring Accounting Settings, page 3-119.

Downloaded from www.Manualslib.com manuals search engine

Configuring Start-Up Settings

Use this option to configure the access point for your network's BOOTP or DHCP servers for automatic assignment of IP addresses.

Procedure

Step 1 Select **Services** > **Start-Up.** The Services: Start-Up dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-30 Start-Up Settings

Field	Description
Configuration Server Protocol	From the list, select one of the following: • None—Use this setting if your network does not have an automatic system for IP address assignment. • BOOTP—Use this setting if IP addresses are hard-coded based on MAC addresses. • DHCP—Use this setting if IP addresses are “leased” for predetermined periods of time.
Use prior Config Server settings if no server responds?	From the list, select one of the following: • yes—Use this setting to have the access point save the boot server's most recent response. • no—Use this setting to not use the most recent response.

Downloaded from www.Manualslib.com manuals search engine

Table 3-30 Start-Up Settings (continued)

Field	Description
Read ".ini" file from file server?	From the list, select one of the following: • always—Use this setting for the access point to always load configuration settings from an.ini file on the server. • never—Use this setting for the access point to never load configuration settings from an.ini file on the server. • if specified by server—Use this setting for the access point to load configuration settings from an.ini file on the server if the server's DHCP or BOOTP response specifies that an.ini file is available.
BOOTP Server Timeout (sec's)	Enter the length of time the access point waits to receive a response from a single BOOTP server.
DHCP Multiple-Offer Timeout (sec's)	Enter the length of time the access point waits to receive a response when there are multiple DHCP servers.
DHCP Requested Lease Duration (min's)	Enter the length of time the access point requests for an IP address lease from your DHCP server.
DHCP Minimum Lease Duration (min's)	Enter the shortest amount of time the access point accepts for an IP address lease. The access point ignores leases shorter than this period.

Downloaded from www.Manualslib.com manuals search engine

Table 3-30 Start-Up Settings (continued)

Field	Description
DHCP Client Identifier Type	From the list, select one of the following: • Ethernet (10Mb) • Experimental Ethernet (3Mb) • Amateur Radio AX.25 • Proteon ProNET Token Ring • Chaos • IEEE 802 Networks • ARCNET • Hyperchannel • Lanstar • AutoNet Short Address • LocalTalk • LocalNet • Other-Non Hardware Click **see details** to see which versions this setting is valid for.

Downloaded from www.Manualslib.com manuals search engine

Table 3-30 Start-Up Settings (continued)

Field	Description
DHCP Client Identifier Value	Use this setting to include a unique identifier in the access point's DHCP request packet. • If you select Other-Non Hardware from the DHCP Client Identifier Type list, you can enter up to 255 alphanumeric characters. • If you select any other option from the DHCP Client Identifier Type list, you can enter up to 12 hexadecimal characters (numbers 0 through 9, and the letters A through F). Click **see details** to see which versions this setting is valid for.
DHCP Class Identifier	Enter the access point's group name. The DHCP server uses the group name to determine the response to send to the access point.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Console/Telnet Settings

Use this option to configure the access point to work with a terminal emulator or through Telnet.

Procedure

Step 1 Select **Services** > **Console/Telnet.** The Services: Console/Telnet dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Downloaded from www.Manualslib.com manuals search engine

Table 3-31 Console/Telnet Settings

Field	Description
Baud Rate	Enter a rate from 110 to 115,200, expressed in bits per second. The rate you enter is dependent on the capability of the computer you use to open the access point management system.
Parity	From the list, select one of the following: • None—Use this setting to use no parity bit. • Even—Use this setting to make the total number of bits even. • Odd—Use this setting to make the total number of bits odd.
Data Bits	From the list, select one of the data bit settings.
Stop Bits	From the list, select one of the stop bit settings.
Flow Control	From the list, select one of the following: • None—Use this setting to indicate no flow control is used. • SW Xonn/Xoff—Use this setting to indicate the method information is sent between pieces of equipment to prevent loss of data when too much information arrives at the same time on one device.
Terminal Type	From the list, select one of the following: • teletype—Use this setting if your terminal emulator does not support ANSI. • ANSI—Use this setting to offer graphic features such as reverse video buttons and underlined links.

Downloaded from www.Manualslib.com manuals search engine

Table 3-31 Console/Telnet Settings (continued)

Field	Description
Columns (64-132)	Enter a number to define the width of the terminal emulator display within the range of 64 characters to 132 characters.
Lines (16-50)	Enter a number to define the height of the terminal emulator display within the range of 16 characters to 50 characters.
Telnet	From the list, select one of the following: • Enable—Use this setting to enable Telnet access to the management system. • Disable—Use this setting to prevent Telnet access to the management system.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Hot Standby Settings

Use this option to configure a standby access point as a client device associated to a monitored access point.

Procedure

Step 1 Select **Services** > **Hot Standby**. The Services: Hot Standby dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-32 Hot Standby Settings

Field	Description
Hot Standby Mode	From the list, select one of the following: • Enable—Use this setting to allow hot standby mode. • Disable—Use this setting to disable hot standby mode.
Service Set ID (SSID)	Enter the monitored access point's SSID.
MAC Address for the Monitored AP	Enter the monitored access point's MAC address.
Polling Frequency (1-30)	Enter the number of seconds between each query the standby access point sends to the monitored access point.
Timeout for Each Polling (1-600)	Enter the number of seconds the standby access point should wait for a response from the monitored access point before it assumes that the monitored access point has malfunctioned.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Configuring Routing Settings

Use this option to configure the access point to communicate with the IP network routing system.

Procedure

Step 1 Select **Services** > **Routing**. The Services: Routing dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-33 Routing Settings

Field	Description
Default Gateway	Enter the IP address of your network's default gateway in this entry field. The entry 255.255.255.255 indicates no gateway.
New Network Route	
Destination Network	Enter the IP address of the destination network.
Gateway	Enter the IP address of the gateway used to reach the destination network.
Subnet Mask	Enter the subnet mask associated with the destination network.

Step 3 Click **Add** to add an additional network route for the access point.

Step 4 To remove a network route, select it from the list, then click **Remove**.

Downloaded from www.Manualslib.com manuals search engine

Step 5 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring CDP Settings

Use this option to enable, disable, or adjust the access point's CDP settings.

Procedure

Step 1 Select **Services** > **CDP**. The Services: CDP dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-34 CDP Settings

Field	Description
Cisco Discovery Protocol (CDP)	From the list, select one of the following: • Enable—Use this setting to enable CDP. • Disable—Use this setting to disable CDP.

Downloaded from www.Manualslib.com manuals search engine

Table 3-34 CDP Settings (continued)

Field	Description
Packet Hold Time	Enter the number of seconds other CDP-enabled devices should consider the access point's CDP information valid.
Packet Sent Every	Enter the number of seconds between each CDP packet the access point sends. This value should always be less than the packet hold time.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring DNS Settings

Use this option to configure the access point to work with your network's Domain Name System (DNS) server.

Procedure

Step 1 Select **Services** > **DNS**. The Services: DNS dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Downloaded from www.Manualslib.com manuals search engine

Table 3-35 DNS Settings

Field	Description
Domain Name System (DNS)	From the list, select one of the following: • Enable—Use this option if your network DNS. • Disable—Use this option if you network does not use DNS.
Default Domain	Enter the name of your network's IP domain. Your entry might look like this: mycompany.com
Domain Name Servers	Enter the IP addresses of up to three domain name servers on your network.
Domain Suffix	Enter the portion of the full domain name that you would like omitted from access point displays.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring FTP Settings

Use this option to configure File Transfer Protocol settings for the access point. All non-browser file transfers are governed by these settings.

Procedure

Step 1 Select **Services** > **FTP**. The Services: FTP dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-36 FTP Settings

Field	Description
File Transfer Protocol (FTP)	From the list select one of the following: • TFTP • FTP
Default File Server	Enter the IP address or DNS name of the file server where the access point should look for FTP files.
FTP Directory	Enter the file server directory that contains the firmware image files.
FTP User Name	Enter the username assigned to your FTP server. You do not need to enter a name in this field if you selected TFTP.
FTP User Password	Enter the password associated with the file server's username. You do not need to enter a password in this field if you selected TFTP.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Configuring HTTP Settings

Use this option to configure HTTP settings for the access point.

Procedure

Step 1 Select **Services** > **HTTP** The Services: HTTP dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-37 HTTP Settings

Field	Description
Allow Non-Console Browsing	From the list, select one of the following: • Enable—Use this setting to allow browsing to the management system. • Disable—Use this setting to make the management system accessible only through the console and Telnet interfaces.
HTTP Port	Enter the port through which the access point provides web access.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Configuring SNMP Settings

Use this option to configure settings for notifications to be sent to an SNMP server.

Procedure

Step 1 Select **Services** > **SNMP**. The Services: SNMP dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-38 SNMP Settings

Field	Description
Simple Network Management Protocol (SNMP)	From the list, select one of the following: • Enable—Use this setting to allow event notifications to be sent to an SNMP server. • Disable—Use this setting to not allow event notifications to be sent to an SNMP server.
SNMP Trap Destination	Enter the IP address or the host name of the server running the SNMP Management software.
SNMP Trap Community	Enter the SNMP community name.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring SNTP Settings

Use this option to configure time server settings.

Procedure

Step 1 Select **Services** > **SNTP**. The Services: SNTP dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-39 SNTP Settings

Field	Description
Simple Network Time Protocol (SNTP)	From the list, select one of the following: • Enable—Use this setting if your network uses Simple Network Time Protocol. • Disable—Use this setting if your network does not use Simple Network Time Protocol.
Default Time Server	Enter enter the server's IP address.

Downloaded from www.Manualslib.com manuals search engine

Table 3-39 SNTP Settings (continued)

Field	Description
GMT Offset (hr.)	From the list, select the time zone in which the access point operates.
Use Daylight Savings Time	From the list, select one of the following: • Enable—Use this setting to have the access point automatically adjust to Daylight Savings Time. • Disable—Use this setting to not have the access point automatically adjust to Daylight Savings Time.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Accounting Settings

Use this option to configure settings that enable you to send network accounting information about wireless client devices to a RADIUS server on your network.

Procedure

Step 1 Select **Services** > **Accounting**. The Services: Accounting dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-40 Accounting Settings

Field	Description
Enable accounting	From the list, select one of the following: • enable—Use this setting to turn on accounting for your wireless network. • disable—Use this setting to turn off accounting for your wireless network
Enable delaying to report STOP	• enable—Use this setting to delay sending a stop report to the server when a client device disassociates from the access point. The delay reduces accounting activity for client devices that disassociate from the access point and then quickly reassociate. • disable—Use this setting to not delay sending a stop report to the server when a client device disassociates from the access point.
Minimum delay time to report STOP (sec)	Enter the number of seconds the access point waits before sending a stop report to the server when a client device disassociates from the access point.
Server Name/IP	Enter the name or IP address of the server to which the access point sends accounting data.

Downloaded from www.Manualslib.com manuals search engine

Table 3-40 Accounting Settings (continued)

Field	Description
Server Type	Select RADIUS from the list. (Additional types may be added in future software releases.)
Port	Enter the communication port setting used by the access point and the server. The default setting, 1813, is the correct setting for Cisco Aironet access points and Cisco secure ACS.
Shared Secret	Enter the shared secret used by your server. It must match the shared secret on the RADIUS server.
Retran (sec)	Enter the amount of time to wait before retransmitting.
Max Retran	Enter the maximum number of times to attempt retransmissions. Click ***** (asterisk) for information on which version this setting is valid.

Downloaded from www.Manualslib.com manuals search engine

Table 3-40 Accounting Settings (continued)

Field	Description
Enable Update	From the list, select one of the following: • enable—Use this setting to allow accounting update messages for wireless clients. With updates enabled, the access point sends an accounting start message when a wireless client associates to the access point, sends updates at regular intervals while the wireless client is associated to the access point, and sends an accounting stop message when the client disassociates from the access point. • disable—Use this setting to not allow accounting update messages. With updates disabled, the access point sends only accounting start and accounting stop messages to the server.
Update Delay (sec's)	Enter the update interval in seconds. If you use 360, the access point sends an accounting update message for each associated client device every 6 minutes.

Downloaded from www.Manualslib.com manuals search engine

Table 3-40 Accounting Settings (continued)

Field	Description
EAP Auth.	From the list, select one of the following: • Yes—Use this server for EAP authentication. In this type of authentication, the access point relays authentication messages between the server and the authenticating client device. • No—Do not use this server for EAP authentication.
Non-EAP Auth.	From the list, select one of the following: • Yes—Use this server for non-EAP authentication. • No—Do not use this server for non-EAP authentication.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Configuring Events

This option enables to you to customize the display of access point events (alerts, warnings, and normal activity).

Procedure

Step 1 Select **Events**. The menu expands and the Events dialog box displays in the right pane.

Step 2 Select one of the following from the Events menu:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Event Handling—See Configuring Event Handling, page 3-124.
- Event Notifications—See Configuring Event Notification, page 3-129.

Configuring Event Handling

The event settings control how events are handled by the access point: counted, displayed in the log, recorded, or announced in a notification. The settings are color coded: red for fatal errors, magenta for alerts, blue for warnings, and green for information.

Procedure

Step 1 Select **Events > Event Handling**. The Events: Event Handling dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-41 Event Handling Settings

Field	Description
System Fatal	From the list, select one of the following: • Count—Use this option to tally the total events occurring in this category without any form of notification or display. • Display Console—Use this option to provide a read-only display of the event but not record it. • Record—Use this option to make a record of the event in the log and provide a read-only display of the event. • Notify—Use this option to makes a record of the event in the log, display the event, and tell the access point to notify someone of the occurrence.
Protocol Fatal	
Network Port Fatal	
System Alert	
Protocol Alert	
Network Port Alert	
External Alert	
System Warning	
Protocol Warning	
Network Port Warning	
External Warning	
System Information	
Protocol Information	
Network Port Information	
External Information	

Downloaded from www.Manualslib.com manuals search engine

Table 3-41 Event Handling Settings (continued)

Field	Description
Handle Alerts as Severity Level	From the list, select one of the following: • systemFatal—Indicates an event that prevents operation of the device as a whole. • protocolFatal—Indicates an event that prevents operation of a specific communications protocol in use, such as HTTP or IP. • portFatal—Indicates an event that prevents operation of the Ethernet or radio network interface. • systemAlert—Indicates that you need to take action to correct a condition on the device as a whole. • protocolAlert—Indicates that you need to take action to correct a condition on a specific communications protocol in use, such as HTTP or IP. • portAlert—Indicates that you need to take action to correct the condition on the Ethernet or radio network interface. • externalAlert—Indicates that you need to take action to correct the condition on a device on the network.

Downloaded from www.Manualslib.com manuals search engine

Table 3-41 Event Handling Settings (continued)

Field	Description
	• systemWarning—Indicates that an error or failure may have occurred on the device as a whole. • protocolWarning—Indicates that an error or failure may have occurred on a specific communications protocol in use, such as HTTP or IP. • portWarning—Indicates that an error or failure may have occurred on an Ethernet or radio network interface. • externalWarning—Indicates that an error or failure may have occurred on a device. • systemInfo—Notification that some sort of event has occurred on a device. • protocolInfo—Notification that some sort of event has ocurred on a communications protocol in use, such as HTTP or IP. • portInfo—Notification that some sort of event has ocurred on an Ethernet or radio network interface. • externalInfo—Notification that some sort of event has ocurred on a device.

Downloaded from www.Manualslib.com manuals search engine

Table 3-41 Event Handling Settings (continued)

Field	Description
Maximum Number of Bytes Stored per Alert Packet (0- 2312)	Enter the maximum number of bytes the access point stores for each Station Alert packet when packet tracing is enabled. If you use 0, the access point does not store bytes for Station Alert packets; it only logs the event. **Note** Changing this setting may cause the access point to reboot.
Maximum Memory Reserved for Detailed Event Trace Buffer (bytes) (0-8388608)	Enter the number of bytes reserved for the Detailed Event Trace Buffer. The Detailed Event Trace Buffer is a tool for tracing the contents of packets between specified stations on your network. **Note** Changing this setting may cause the access point to reboot.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Downloaded from www.Manualslib.com manuals search engine

Configuring Event Notification

Use this option to enable and configure notification of fatal, alert, warning, and information events to destinations external to the access point, such as an SNMP server or a Syslog system.

Procedure

Step 1 Select **Events** > **Event Notification**. The Events: Event Notification dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-42 Events > Event Notification Settings

Field	Description
Should Notify-Disposition Events generate SNMP Traps?	From the list, select one of the of the following: • Yes—Use this option to send event notifications to an SNMP server. • No—Use this option if you do not want to send notifications to an SNMP server.
SNMP Trap Destination	Enter the IP address or the host name of the server running the SNMP Management software.
SNMP Trap Community	Enter the SNMP community name.
Should Notify-Disposition Events generate Syslog Messages?	From the list, select one of the of the following: • Yes—Use this option to send event notifications to a Syslog server. • No—Use this option if you do not want to send notifications to a Syslog server.

Downloaded from www.Manualslib.com manuals search engine

Table 3-42 Events > Event Notification Settings (continued)

Field	Description
Syslog Destination Address	Enter the IP address or the host name of the server running Syslog.
Syslog Facility Number	Enter the Syslog Facility number for the notifications.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Custom Values

This option enables to you to enter custom values that might not be available in the Template Menu. It also allows you to quickly enter a value, if you know the exact value you want to change, instead of going through the menu.

Note This option should be used only by advanced users who have a good understanding of the MIB variables they are setting.

Templates with custom key values are not validated.

Procedure

Step 1 Select **Configure** > **Templates** > **Custom Values**. The Custom Values dialog box appears.

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Complete the following:

Note You must enter the exact syntax for the setting to work properly.

Field	Description
Key	Enter a valid MIB key.
Value	Enter a valid MIB value.

Step 3 Click **Add** to add the custom value to the list.

Note If the custom value you enter is the same as an existing one in the Template Menu, the custom value will override the value in the menu.

Step 4 To remove a custom value, select it from the list, then click **Remove**.

Step 5 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-131.)
- **Finish** to save the template. (See Finishing the Template, page 3-132.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Previewing the Template

Procedure

Step 1 Click **Preview.** A window displays the configuration choices you have made to the template.

Step 2 Click Finish. (See Finishing the Template, page 3-132.)

Downloaded from www.Manualslib.com manuals search engine

Finishing the Template

Procedure

Step 1 Click **Finish** in the left pane to complete creating a template. The Finish dialog box appears in the right pane.

Note It is recommended that you always validate the template before saving it.

Step 2 Click **Validate** if you want to check the template configuration. A window displays a message indicating for which devices and versions the configuration template you just created is valid.

Note Templates containing custom key values are not validated.

Step 3 Check **Enable Version Checking** if you want the system to make sure you apply the templates only to devices with valid versions.

If you do not enable the version check, templates will be applied to devices even when the configuration is not valid for the device version.

Step 4 Click **Save** to create the template. The screen refreshes and the template name appears in the Existing Templates listbox.

Creating a Template

Use this option to create a configuration template.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure** > **Templates**. The Templates dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Enter a unique name. (See Naming Guidelines, page A-1 for details.)

Step 3 Click **Create New**. The window refreshes with Template Creation menu in the left pane and the Template Name dialog box in the right pane.

Step 4 Select the choices in the left pane to create a configuration template. For a description, see Template Choices, page 3-2.

Copying a Template

Use this option to copy a configuration template that you can use as a base for another template.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure** > **Templates**. The Templates dialog box appears.

Step 2 Select the template you want to copy from the Existing Templates box, then click **Create Copy**. A dialog box appears asking you to enter a name for the copy.

Step 3 Enter a unique name. (See Naming Guidelines, page A-1 for details.)

Step 4 Click **OK**. The Templates window refreshes and the new name appears in the Existing Templates list.

Step 5 Click **Edit.** (See Editing a Template, page 3-134.)

Downloaded from www.Manualslib.com manuals search engine

Editing a Template

Use this option to edit a configuration template.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure** > **Templates**. The Templates dialog box appears.

Step 2 Select the template you want to edit from the Existing Templates box, then click **Edit**. The window refreshes with Template Creation menu in the left pane and the Template Name dialog box in the right pane.

Step 3 Select the choices in the Template Menu to create a configuration template. For a description, see Template Choices, page 3-2.

Deleting a Template

Use this option to delete a configuration template.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure** > **Templates**. The Templates dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Select the template you want to delete from the Existing Templates box, then click **Delete**. A window appears asking if you want to delete the template.

Note You cannot delete a template if it used in a scheduled job.

Step 3 Click **OK** to delete it.

Importing a Template

Use this option to import a configuration to the WLSE, either from a file or from a device. You can import files from devices that are not managed by the WLSE.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure** > **Templates**. The Templates dialog box appears.

Step 2 Click **Import**. The Import Template window appears.

Step 3 Complete the following:

Field	Description
Template Name	Enter a name for the template.
Description	Enter a description for the template
From file	Enter the template filename or browse to find the file, then click **Import**.
From device (IP Address)	Enter a device name or IP address, then click **Import**.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Non-IP-Identity	Select this option if you do not want to download identity parameters, such as IP address, from the access point. Some parameters are ignored using this type of import. The downloaded configuration parameters are not a full representation of the access point's configuration but an optimal representation.
Full	Select this option to import a full configuration from the access point. This type of import includes the access point's identity parameters, such as sysname, IP address, etc. **Note** When using this option, it is recommended you delete all the custom key values from the imported template before applying the template to any device.
Device Credentials	
User Name	If the device is not managed by the WLSE, or if the device is managed but the credentials have not been set, enter the username on the access point.
User Password	If the device is not managed by the WLSE, enter the user password on the access point.

Step 4 To import another template, click **Back** and repeat Step 3.

Step 5 When you are finished, click **Done.**

Step 6 View the template you imported by selecting **Configure** > **Templates** and selecting it in the Existing Templates list.

Downloaded from www.Manualslib.com manuals search engine

Note Any configuration options in the imported file, which cannot be configured using the WLSE, will appear in Custom Values. It is recommended that you delete the custom values.

Exporting a Template

Use this option to export a configuration template to your local drive.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure** > **Templates**. The Templates dialog box appears.

Step 2 Select a template name from Existing Templates, then click **Export**. The Export Template window appears.

Step 3 From the list, select the template you want to export, then click **Export**. You will be prompted for a location to export the.ini file.

Step 4 Click **Done**.

Managing Configuration Jobs

This is window allows you view a list of all the jobs in their various states. It also allows you to create, edit, and filter, and undo configuration jobs.

The topics covered in this section are:

- Creating a Configuration Job, page 3-144
- Viewing Configuration Job Status, page 3-144
  - Filtering a Job, page 3-147
  - Editing a Job, page 3-148

Downloaded from www.Manualslib.com manuals search engine

- Deleting a Job, page 3-148
- Copying a Job, page 3-148
- Viewing Job Run Details, page 3-149

Related Topic

Using the Templates, page 3-1.

Job Choices

When you create or edit a configuration job, the following choices appear in the left pane of the Jobs window:

Note All these steps, except Schedule Job, must be completed but do not have to be done in order. You schedule a job later.

1. **Job Name**—See Naming the Job, page 3-138.
2. **Select Devices**—See Selecting Devices, page 3-139.
3. **Select Template**—See Selecting a Template, page 3-140.
4. **Schedule Job**—See Scheduling a Job, page 3-142.
5. **Finish**—See Finishing the Job, page 3-143.

Caution Clicking on another Configure subtab before you have saved your entries in this window will cause the window to reset and you will lose all the information you entered.

Naming the Job

Procedure

Step 1 Click **Job Name.** The Job Name dialog box appears.

Step 2 Complete the following:

Downloaded from www.Manualslib.com manuals search engine

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 3-43 Job Name

Field	Description
Job Name	Enter a name for the job. See Naming Guidelines, page A-1.
Description	Enter a description of the job. See Naming Guidelines, page A-1.
Protocol	Select the type of protocol used: HTTP or SNMP.

Step 3 From the menu in the left pane, go to the next step, Select Devices. (For additional information, see Selecting Devices, page 3-139.)

Selecting Devices

Procedure

Step 1 Click **Select Devices.** The Select window appears.

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Step 2 From the device selector, click the folder from which you want to build a device list.

- Clicking the folder displays the folder's contents in the Available Devices list box.
- Repeat this step as many times as necessary to select devices from the folder in which they reside.

Downloaded from www.Manualslib.com manuals search engine

Step 3 From the Available Devices list, select folders or individual devices, then click **Add**. The devices appear in the Selected Devices list box.

Note If you select a folder, the template will be applied to all of the devices in that folder. If a device is subsequently added to the folder, the template is applied to that device.

Step 4 To remove devices, select them from the Devices in Group list, then click **Remove**.

Step 5 From the menu in the left pane, go to the next step, Select Template. (For additional information, see Selecting a Template, page 3-140.)

Selecting a Template

Procedure

Step 1 Click **Select Template.** The Select Template window appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 3-44 Select Template

Field	Description
Configuration Template	From the list, select the template which you want to apply to the devices.
Details	
Name	Displays the name of the selected template.
Device Types	Displays the device types that are valid for the selected template.
Device Versions	Displays the device versions for the device types listed in the Device Type field. Each device type's valid versions are displayed in sequence and grouped using parentheses.
Description	Displays the template description.
Version Check Enabled	Indicates whether the version check is enabled. (The check is enabled using the Finish step in the Template Menu.)

Step 3 From the menu in the left pane, go to the next step, Schedule Job. (For additional information, see Scheduling a Job, page 3-142.)

Downloaded from www.Manualslib.com manuals search engine

Scheduling a Job

Procedure

Step 1 Click **Schedule Job.** The Schedule Job dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 3-45 Schedule Job

Field	Description
Run Now	Click to run the job. **Note** This option ignores any dates you have entered in Start Date and Start Time.
Start Date	From the lists, select the month, day, and year you want your job to run.
Start Time	From the list, select the hour and minutes of the day you want your job to run.
Repeat	
Enable	Check to run the job repeatedly.
Every	Indicate how often you want the job to repeat by entering a numerical value, then selecting an interval of time: Hours, Days, Months, or Years.

Step 3 From the menu in the left pane, go to the next step, Finish. (For additional information, see Finishing the Job, page 3-143.)

Tip You can stop a running job by clicking **Stop Job**.

Downloaded from www.Manualslib.com manuals search engine

Finishing the Job

Procedure

Step 1 Click **Finish** in the left pane to complete creating a job. The Finish dialog box appears in the right pane.

Step 2 If you want email notification of job completion, use the Email settings section:

Field	Description
On completion, email to	Enter a comma-separated list of email addresses to be notified when the job completes.
Email only if job fails	Select this checkbox if you want recipients to be notified only if the job fails.

Tip If email notification is not working, you may need to configure the mailroute by selecting **Administration > Appliance > Configure Mailroute**.

Step 3 Click **Validate** if you want to check the job.

Note Jobs with templates containing custom key values are not validated.

A window displays a confirmation message if the job is successful, and an informational message if the selected template in the job is not valid for the selected devices.

Note It is recommended that you always validate a job before saving it, and to eliminate any errors before saving it. If a job is saved with errors, the devices associated with the errors are ignored when the job runs.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Click **Save** to create the job. The screen refreshes and

- The job name appears in the Scheduled Jobs list.
- A confirmation window appears with the job summary.

Creating a Configuration Job

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure** > **Jobs**. The Jobs window appears.

Step 2 Enter a name for the job. See Naming Guidelines, page A-1.

Step 3 Click **Create Job.** The window refreshes with Job Creation menu in the left pane and the Job Name dialog box in the right pane.

Step 4 Select the numbered choices in the left pane to create a job. For a description, see Job Choices, page 3-138.

Viewing Configuration Job Status

This is window allows you to view job status. It also allows you to filter a job, edit a job, view details about the job and undo a job.

Device data is polled is every 15 minutes by default, and the duration that job data is retained is 30 days. To change either default, see Managing System Parameters, page 6-73.

The topics covered in this section are:

- Viewing the Job, page 3-145
- Filtering a Job, page 3-147
- Editing a Job, page 3-148

Downloaded from www.Manualslib.com manuals search engine

- Deleting a Job, page 3-148
- Copying a Job, page 3-148
- Viewing Job Run Details, page 3-149

Note Your login determines whether you can use this option.

Related Topic

Using the Templates, page 3-1

Viewing the Job

Procedure

Step 1 Select the status of the job you want to view from the Job State list.

Step 2 Select the type of job you want to view from the Job Type list.

Step 3 Click **Apply**. The window refreshes and the jobs are displayed.

The tables vary depending on the type of Job State and Job Type you selected: Scheduled and Unscheduled, Running, or All.

- Scheduled and Unscheduled

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Next Schedule	For scheduled jobs, this indicates the next time the job will run. For completed jobs, this is last time the job ran.
Last Run Status	The status of the last run. **Note** Jobs that cause an access point to reboot are listed as Unverified.

Downloaded from www.Manualslib.com manuals search engine

- Running

Tip You can stop a running job by clicking **Stop Job**.

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Job Start Time	The time the job started.
Percent Complete	The percent of the job that has completed running.
Next Schedule	The next time the job is scheduled to run.

- All

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Job State	The state of the job. **Note** A job in a DidNotStart state must be rescheduled.
Next Schedule	For scheduled jobs, this indicates the next time the job will run. For completed jobs, this is last time the job ran.
Last Run Status	The status of the job the last time it run. **Note** Jobs that cause an access point to reboot are listed as Unverified.

Step 4 To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Downloaded from www.Manualslib.com manuals search engine

Step 5 You can do the following:

Note If the option is not available for the job type, the buttons are grayed.

a. Filter the job—See Filtering a Job, page 3-147.
b. Edit the job—See Editing a Job, page 3-148.
c. Delete the job—See Deleting a Job, page 3-148,
d. Copy a job—See Copying a Job, page 3-148.
e. View the run details—See Viewing Job Run Details, page 3-149.
f. Refresh the screen—Click **Refresh**.

Filtering a Job

Use this option to filter jobs from the displayed list. Filtering this way allows you to display a limited set of jobs, making it easier to search for a particular job if you know the name.

Procedure

Step 1 Click **Filter Job.** The Filter Job dialog box appears.

Step 2 Enter the name, or part of the a name, on which to filter. (Use % as a wildcard to filter jobs. For example, entering %name% will filter all the jobs that contain "name.")

Step 3 Click **Apply filter.** The Job window refreshes and the matching jobs are displayed on the Jobs list.

Note The filter is only applied until the page is refreshed.

Downloaded from www.Manualslib.com manuals search engine

Editing a Job

Use this option to edit jobs from the displayed list of jobs.

Procedure

Step 1 Select the job from the list which you would like to edit.

Step 2 Click **Edit Job.** The Job Name dialog box appears.

Step 3 Select the choices in the Template Menu to create a configuration template. For a description, see Job Choices, page 3-138.

Deleting a Job

Use this option to delete jobs from the displayed list of jobs. Jobs that are scheduled, unscheduled, completed and did not start can be deleted. Jobs that are running cannot be deleted; they can be stopped.

Procedure

Step 1 Select the job from the list which you would like to edit.

Step 2 Click **Delete Job.**

Copying a Job

Use this option to copy unscheduled jobs from the displayed list of jobs, which can be run later on demand.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select the job from the list which you would like to copy.

Step 2 Click **Copy Job.** A dialog box appears.

Step 3 Enter a name for the job, then click **OK.** The screen refreshes and the job is listed.

Viewing Job Run Details

Use this option to view details about a job, or to undo a job from the displayed list of jobs.

Procedure

Step 1 From the table displayed in **Configure > Jobs** window, select a job for which you would like to see details, then click **Job Run Detail**.

Step 2 The details window appears with the Job Runs table:

Field	Description
Select Run	Used to select a job for which you want to see more details.
Job Start Time	The time the job started.
Job End Time	The time the job ended.
Job Status	The status of the job.
Percent Complete	The percent of the job that completed.

Step 3 Do any of the following:

- To view details for a particular job run or to undo a job, select the job, then click **Show Run Details**. The Job Run details table displays the information. (See Viewing the Job Run Details Table, page 3-150.)

Downloaded from www.Manualslib.com manuals search engine

- To view the job run log, click **Job Run Log**. A window displays all the details for the selected job number.
- To refresh the table, click **Refresh**.

Viewing the Job Run Details Table

The Job Runs Details table displays the following information:

Field	Description
Device Name	The name of the device.
Start Time	The time the job started.
End Time	The time the job ended.
Status	The status of the job.

- To sort table data, click on the column heading by which you want to sort the data:
  - A triangle indicates ascending order.
  - An upside-down triangle indicates descending order.
  - No triangle indicates that the data is not sorted.
- To select all the jobs in the table, click **Select All.**
- To deselect all the jobs in the table, click **DeSelect All**.

Note If you have multiple screens, you must Select All or DeSelect All one screen at a time.

Downloaded from www.Manualslib.com manuals search engine

- To undo the selected configuration job, click **Undo**.

  The Undo feature is not supported for the following:

  – Custom Values

  – Security options: Local Admin Authentication under the Local Admin Access; Encryption Key Values under Local AP/Client Security; Shared Secret under Server-Based Security; and Shared Secret under Accounting.

  – FTP username and password

  – Previously undone jobs

  – Routing table configurations (for versions prior to 11.23T only)

  – Adding a user in place of an existing user on the access point. The Undo feature works for new users.

Automating Configurations

This window allows you to automatically upload configuration templates to access points and bridges. Use this feature to:

- Apply startup templates through the DHCP server to newly-installed devices with manufacturer-default configurations.
- Apply a common template to devices after they are discovered, auto managed, and the WLSE has their inventory information.

The topics covered in this section are:

- Assigning a Startup Configuration, page 3-151
- Assigning an Auto-Managed Configuration, page 3-154

Assigning a Startup Configuration

The startup configuration is used for newly-installed devices that have a manufacturer-default configuration. After the devices are powered on and receive an IP address from a DHCP server, the startup configuration will be automatically uploaded to the devices.

Downloaded from www.Manualslib.com manuals search engine

Before You Begin

1. Create a template for the startup configuration. (See Creating a Startup Configuration Template, page 3-153.)
2. Configure the DHCP server to:
   a. Return the WLSE's address. This is done by entering the `<IP address of the WLSE>` in the Boot Server **Host Name** field (option number 066) on the DHCP server.
   b. Return the name of the initial template file in the DHCP reply message. This is done by entering `<startup file name>` in the **BootfileName** field (option number 067) on the DHCP server.

   For example, if you had a WLSE with the IP address 10.10.11.12) and an associated startup template with Bootfile Name "newap1200.ini", you would do the following:
   a. On the DHCP server, select **Scope** > **Scope Options**.
   b. Set Scope option 066 (TFTP boot server name or IP address) with **`10.10.11.12`** (the WLSE's IP address).
   c. Set Scope option 067 (Bootfile Name) with **`new-ap1200.ini`** (the new Bootfile Name associated with the startup template file.)

Tip After the access point is powered on and the startup configuration is applied, you may want to prevent the startup configuration from being uploaded to devices again if for some reason the access points reboot. To prevent the initial configuration from being uploaded to devices after a reboot, set the **bootconfigReadINI** variable on the access point to **never** by auto-managed configuration or regular configuration.

Related Topics

- Creating a Startup Configuration Template, page 3-153
- Assigning an Auto-Managed Configuration, page 3-154

Procedure

Step 1 Select **Configure** > **Auto Update** > **Startup Configuration**. The Startup Configuration Template dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Complete the following:

Field	Description
Startup Templates	Lists the startup templates that have been created.
Bootfile Name	Enter the configuration file name that appears on the DHCP server. This must have an .ini extension.
Description	Enter a description for the configuration.
Configuration Template	From the list select the startup template to assign to the configuration file. Click **Details** to see the device types and device versions for which the template is valid.

Step 3 Click **Save** to save the template.

Step 4 Click **Delete** to delete the template.

Creating a Startup Configuration Template

The startup configuration is used to bootstrap a device to allow the WLSE to discover it.

Caution The startup configuration template is placed in tftpboot directory and anyone who knows the file name can access it. This template should contain only minimal feature settings.

To create a startup template select **Configure** > **Templates**. (To configure the access point manually without using a startup configuration, see Set Up Access Points and Bridges, page 6-12.)

Use the following table to guide you in creating a startup configuration template:

Downloaded from www.Manualslib.com manuals search engine

Tasks	Template Choice	Notes
1. Enable Cisco Discovery Protocol (CDP).	Select **Services** > **CDP**.	CDP is required for the WLSE to discover devices on the network.
2. Enable SNMP. (Optional) Set the location. (Optional) Set the system name and system contact.	Select **Services** > **SNMP**.	SNMP is required for the WLSE to discover and manage the device. Setting the location enables proper grouping of devices into the system-defined Location group. For more information, see Managing Groups, page 6-37.
3. Set the community string by creating a user with all privileges.	Select **Security** > **Local Admin Access.** To create an user with SNMP read/write privileges, enter a username and password and select the Write, SNMP, Firmware, and Administrator capabilities.	The username of the user with Write and SNMP privileges is used as the SNMP read/write community string. This community string should also have been configured on the WLSE using **Administration** > **Discover** > **Device Credentials** > **SNMP Communities**. The Firmware privilege is required for configuring devices from the WLSE.
5. Set up TFTP as the transfer protocol between the WLSE and access points.	Select **Services** > **FTP**.	TFTP is used for transferring configuration changes to access points.

Assigning an Auto-Managed Configuration

Use this option to automatically apply a customized configuration to auto-managed devices after their inventory information has been collected by the WLSE.

The configuration which is applied to the devices is based on the system-defined group with which the devices are associated.

Downloaded from www.Manualslib.com manuals search engine

Tip It is recommended that as part of the auto-managed configuration template, you create an HTTP user and password by selecting **Security > Local Admin Access.** You also enter this user and password on the WLSE by selecting **Administration > Discover > Device Credentials > HTTP User/Password.**

Downloaded from www.Manualslib.com manuals search engine

There following topics are covered in this section:

- Assigning a Configuration Template—See Assigning Auto-Managed Configurations, page 3-156
- Emailing the Configuration Job Results—See Using Auto-Managed Options, page 3-157

Assigning Auto-Managed Configurations

Procedure

Step 1 Select **Configure** > **Auto Update** > **Auto-Managed Configuration**. The Auto-Managed Configuration Templates dialog box appears with the names of the groups for which you can apply an automated template.

Step 2 Complete the following:

Field	Description
Auto-Managed Templates	Lists the auto-managed templates that have been created.
Name	Enter a name for the auto-managed configuration. This must have a .ini extension.
Description	Enter a description for the configuration.
Automatically apply configuration template to devices matching the criteria below when they get auto managed	1. Select the checkbox if you want to automatically apply a template. 2. From the list select the template you want to assign. 3. Click **Details** to see the device types and device versions for which this template is valid.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Device Types	**Note** Auto-managed templates for AP 350's are applied to 350 bridges; you cannot assign a different template for bridges based on device type alone. If the bridges are running are different software version than the AP350s, use a different template for bridges and set the appropriate version numbers. 1. Select the checkbox to enable the device types. 2. From the list, select the device and click >> to add it to the list of valid devices for that template. 3. To remove devices from the list, select the device, then click **Remove**.
Software Versions	1. Select the checkbox to enable the software versions. 2. Enter the version numbers if they are not in the list, or from the list, select the version number, then click >> to add it to the list of valid versions for that template. 3. To remove version numbers, select the version number form the list, then click **Remove.**

Step 3 Click **Save** to save the template.

Step 4 To delete a template, select it from the Auto-Managed Templates listbox, then click **Delete**.

Using Auto-Managed Options

This option allows you to email the results of your auto-managed configuration job.

Procedure

Step 1 Select **Configure** > **Auto Update** > **Auto-Managed Configuration** > **Auto-Managed Options**. The Auto-Managed Configuration Options dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Select the checkbox to enable email notification.

Step 3 Enter the email address for the recipients of the notification.

Tip If email notification is not working, you may need to configure the mailroute by selecting **Administration > Appliance > Configure Mailroute**.

Step 4 Click **Save**.

Downloaded from www.Manualslib.com manuals search engine

Updating Device Firmware

From the WLSE, you can update (or downgrade) firmware on Cisco Aironet 1200 series, 340 series, and 350 series access points and on Cisco Aironet 350 series bridges. The Firmware tab allows you to:

- Import firmware to the WLSE and manage the firmware stored on the WLSE.
- Upload firmware from the WLSE to access points and bridges.
- Use a TFTP server to update access points and bridges in remote locations

The subtabs under Firmware are:

- Images—See Managing Firmware Images, page 4-1
- Jobs—See Managing Firmware Jobs, page 4-9

Note One or both of these subtabs may not be visible to some users.

Managing Firmware Images

The options under the Images subtab allow you to import images to the WLSE from the client desktop or from Cisco.com and manage the images on the WLSE. This section contains information about:

- Viewing images—See Viewing Images on the WLSE, page 4-2
- Editing images—See Editing Image Details on the WLSE, page 4-3
- Deleting images—See Deleting Images from the WLSE, page 4-4

Downloaded from www.Manualslib.com manuals search engine

- Importing images—See Importing Images, page 4-4
- Downloading images to a remote TFTP server—See Using a Remote TFTP Server for Image Upload, page 4-9

Related Topic

Managing Firmware Jobs, page 4-9

Viewing Images on the WLSE

You can view a list of images stored on the WLSE or view details on selected images.

Procedure

Step 1 Select **Firmware > Images**. The Firmware Images selector appears, showing the images that have been downloaded to the WLSE.

Step 2 To view the list of available images for a type of device, expand its folder.

Note Images that you download to the WLSE are automatically listed in the Firmware Images selector.

Step 3 To view details on an image, select the image. The Image Details window opens, showing the image name, image version, image size, and a description.

Related Topic

Editing Image Details on the WLSE, page 4-3

Downloaded from www.Manualslib.com manuals search engine

Editing Image Details on the WLSE

Procedure

Step 1 Select **Firmware** > **Images**. The Firmware Images selector appears.

Step 2 Expand the folder that contains the image you want to edit, then select the image. The Image Details window opens.

Step 3 You can edit the image name, image version, device type, and description:

Table 4-1 Image Details

Field	Description
Name	By default, the name of the image file or of the image file in a zipped file.
Device Type	The device type to which the firmware applies. If you change the device type of an image, the image is removed from the former device type folder and added to the new one. For example, if you change the device type from AP340 to AP350, the image is removed from the AP340 folder and added to the AP350 folder.
Version	The image version. Be careful when changing the version; proper uploading of firmware to devices requires accurate version information. You can enter the version in uppercase or lowercase.
Size	Size of the image (read-only field).
Description	This field is blank by default.

Step 4 When you finish editing, click **Save**.

Related Topic

Deleting Images from the WLSE, page 4-4

Downloaded from www.Manualslib.com manuals search engine

Deleting Images from the WLSE

Procedure

Step 1 Select **Firmware** > **Images**. The Firmware Images selector appears.

Step 2 Expand the folder that contains the image you want to delete, then select the image. The Image Details window opens.

Step 3 Click **Delete**, then click **OK**. The image is deleted from the list of images in the folder.

Related Topics

- Viewing Images on the WLSE, page 4-2
- Editing Image Details on the WLSE, page 4-3

Importing Images

This option allows you to:

- Download images to the WLSE from the desktop—see Importing Images from the Client System Desktop to the WLSE, page 4-5.
- Download images to the WLSE directly from Cisco.com—see Importing Images Directly from Cisco.com to the WLSE, page 4-7.

Note Even if you are uploading images from a remote TFTP server, you must still import the images to the WLSE.

Related Topics

- Viewing Images on the WLSE, page 4-2
- Editing Image Details on the WLSE, page 4-3

Downloaded from www.Manualslib.com manuals search engine

Importing Images from the Client System Desktop to the WLSE

Procedure

Step 1 Download the desired firmware images to your client system from Cisco.com. You can download firmware images from the following URL:

http://www.cisco.com/public/sw-center/sw-wireless.shtml

Note Only the combined images from Cisco.com are supported for importing to the WLSE. If you download an image component from another site and then try to import a component, the operation will fail.

For information about supported versions of images, see the WLSE Supported Devices Table on Cisco.com.

Step 2 Select **Firmware > Images > Import > From Desktop**. The Desktop Image window appears. Complete the following:

Table 4-2 Desktop Import Window

Field	Description
Device Type	Select the device type from the list.
Version	Enter the image version. Be careful when entering the version; proper uploading of firmware to devices requires accurate version information. You can enter the version in uppercase or lowercase characters.

Downloaded from www.Manualslib.com manuals search engine

Table 4-2 Desktop Import Window (continued)

Field	Description
File Location	Enter the path to the image on the client system or click **Browse**. Images for Cisco Aironet 350 wireless bridges may be named as images for access points (that is, names begin with *AP*). To avoid confusion, you can rename these images (see Editing Image Details on the WLSE, page 4-3.)
Overwrite Existing Image	Select this checkbox if you are importing an image that is already stored on the WLSE. Otherwise, the image import will fail if the same image is already stored on the WLSE.

Note If the image file is in zip format, it will be automatically unzipped during the import operation.

Step 3 Click **Import**. An informational popup window appears. *Do not close the popup window until you receive a message that the import was successful or the import failed.*

If the import is successful, a confirmation message appears and the image is saved on the WLSE.

If the import fails, an error message appears. The import may fail for one of the following reasons:

- The image you are trying to import is not valid. An error message appears.
- There is insufficient space on the WLSE to store images.
- You specified an image that already exists in the image library and you did not select the Overwrite Existing Image checkbox in Step 2.

Step 4 Repeat Steps 2 and 3 to import more images.

Step 5 For information on uploading firmware to access points and bridges, see Managing Firmware Jobs, page 4-9.

Downloaded from www.Manualslib.com manuals search engine

Importing Images Directly from Cisco.com to the WLSE

Procedure

Step 1 Select **Firmware > Images > Import > From Cisco.com**. The Cisco.com Import window is displayed. Complete the following:

Table 4-3 Cisco.com Import Window

Field	Description
Cisco.com Username	Your Cisco.com username.
Cisco.com Password	Your Cisco.com password
Proxy IP/Hostname [1]	The IP address or hostname of the proxy server used to mediate between the web browser and Cisco.com and the proxy port used by the proxy server (if required on your network).
Proxy Port	
Proxy Username	The username and password for contacting the proxy server (if required on your network).
Proxy Password	

1. Some proxy server software does not work properly with importing firmware from Cisco.com. If you have problems using your proxy server with this feature, download the firmware image to your desktop from Cisco.com and import the image from the desktop (see Importing Images from the Client System Desktop to the WLSE, page 4-5).

Step 2 To clear all of your entries in the window, click **Clear**.

Step 3 To log into Cisco.com, click **Login**. The Cisco.com Import window changes to allow you to view the firmware images available on Cisco.com.

Step 4 Click one of the entries in the Device Type column; the firmware versions available on Cisco.com are displayed. Select a firmware version from the entries in the Versions column; the image details are displayed, along with the **Add** button.

Downloaded from www.Manualslib.com manuals search engine

Note Images for Cisco Aironet 350 wireless bridges are listed in the Import window as Cisco Aironet 350 access point images (that is, the names begin with *AP*). To avoid confusion, you can rename these images after importing them. For more information, see Editing Image Details on the WLSE, page 4-3.

Step 5 To add the image to the Selected Images list, click **Add**.

Step 6 Repeat steps 4 and 5 to add more images.

Step 7 To remove an image from the Selected Images list, click **Remove**.

Select the Overwrite Existing Images checkbox if you are importing an image version that is already stored on the WLSE. Otherwise, the image import will fail if the same version is already stored on the WLSE.

Step 8 Click **Import**. An informational popup window appears. *Do not close the popup window until you receive a message that either says the import was successful or the import failed.*

If the import is successful, a confirmation message appears and the image is saved on the WLSE.

If the import fails, an error message appears. The import may fail for one of the following reasons:

- The image you are trying to import is not valid. In that case, an error message appears.
- There is insufficient space on the WLSE to store images.
- You specified an image that already exists in the image library and you did not select the Overwrite Existing Image checkbox in Step 7.

Step 9 For information on uploading firmware to access points and bridges, see Managing Firmware Jobs, page 4-9.

Downloaded from www.Manualslib.com manuals search engine

Using a Remote TFTP Server for Image Upload

You can download firmware images to a TFTP server and then upload them to access points and bridges. This method of uploading may be quicker than uploading from the WLSE if you have a slow link between the WLSE and the access points and bridges in your network.

To download firmware images, go to the following URL:

http://www.cisco.com/public/sw-center/sw-wireless.shtml

To make sure you are downloading a supported firmware release, see the Supported Devices Table for the CiscoWorks 1105 Wireless LAN Solution Engine on Cisco.com.

Use the normal procedure for creating firmware jobs described in Managing Firmware Jobs, page 4-9. You specify the TFTP server and provide the filename in the last step; see Finishing the Job, page 4-14.

Note Even though you may be uploading images from a remote TFTP server, you still need to import those images to the WLSE. For information on importing images to the WLSE, see Importing Images, page 4-4.

Managing Firmware Jobs

This window allows you view a list of all the firmware jobs in their various states. It also allows you to create, edit, filter, and delete firmware jobs.

The topics covered in this section are:

- Creating a Firmware Job, page 4-18
- Using the Job Functions, page 4-18
  - Viewing Jobs by Job State, page 4-19
  - Filtering Jobs, page 4-21
  - Editing a Job, page 4-21
  - Deleting a Job, page 4-22
  - Viewing Job Run Details, page 4-22

Downloaded from www.Manualslib.com manuals search engine

Related Topic

Managing Firmware Images, page 4-1

Job Choices

When you create or edit a firmware upload job, the following tasks appear in the left pane of the Jobs window. These tasks must be completed whether you are uploading images from the WLSE or from a remote TFTP server. You can omit scheduling the job and edit the job later to provide a schedule. You can complete tasks 1 through 4 in any order.

1. **Job Name**—See Naming the Job, page 4-10.
2. **Select Image**—See Selecting the Image, page 4-11.
3. **Select Devices**—See Selecting Devices, page 4-12.
4. **Schedule Job**—See Scheduling the Job, page 4-13.
5. **Finish—**After completing tasks 1 through 4, you validate and save the job—See Finishing the Job, page 4-14.

Caution Clicking on a any subtab (for example, Jobs or Images) before you have saved your entries in the Jobs window will cause the window to reset and you will lose all the information you entered.

Naming the Job

Procedure

Step 1 Click **Job Name.** The Job Name dialog box appears.

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Complete the following:

Table 4-4 Job Name Parameters

Field	Description
Job Name	Enter a name for the job. For guidelines on naming jobs, see Naming Guidelines, page A-1.
Description	Enter a description of the job. For guidelines on entering descriptions, see Naming Guidelines, page A-1.
Protocol	Select the protocol to be used for the job: HTTP or SNMP.

Step 3 From the menu in the left pane, go to the next step, Select Image. See Selecting the Image, page 4-11.

Selecting the Image

Procedure

Step 1 Click **Select Image**. The Firmware Images selector appears.

Step 2 Expand the device folder and select the image you want to upload. The Image Detail window opens.

If the desired image does not appear, you must import it to the WLSE. For more information, see Importing Images, page 4-4.

Step 3 From the menu in the left pane, go to the next step, Select Devices. See Selecting Devices, page 4-12.

Downloaded from www.Manualslib.com manuals search engine

Selecting Devices

Procedure

Step 1 Click **Select Devices.** The Select Devices window appears. All managed devices are listed in the Device selector in the middle pane.

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Step 2 To search for devices:

a. From the list in the search area located in the middle pane, select the method for searching: by device name or IP address.

b. Enter the IP address or name. You can use asterisks (*) as wildcards. An asterisk denotes any number of characters in a name or an entire octet in an IP address; for example, *AP or 172.*.*.*.

c. Click **Go**. The matching devices appear in the Search Results folder in the device selector.

Step 3 To select devices for image upload, expand a folder that contains the devices you want to include in the job. Then click the device group folder. The group and all its devices are added to the Available Devices list.

For more information on device grouping, see Managing Groups, page 6-37.

Step 4 From the Available Devices list, select a group or individual devices, then click **Add**. The devices appear in the Selected Devices list box.

The devices in the Selected Devices list box will receive the image you select.

Step 5 To add devices from other groups, repeat steps 3 and 4.

Step 6 To remove devices, select them from the Selected Devices list, then click **Remove**.

Step 7 From the menu in the left pane, go to the next step, Schedule Job. See Scheduling the Job, page 4-13.

Downloaded from www.Manualslib.com manuals search engine

Related Topic

Managing Groups, page 6-37

Scheduling the Job

When scheduling a firmware job, you can select Run Now to start the job in 2 minutes, or you can schedule the job for a future date and time.

Note You can save a job without scheduling it. You can edit the job later to add the scheduling information.

Procedure

Step 1 Click **Schedule Job.** The Schedule Job dialog box appears.

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Step 2 Schedule the job as follows:

- To run the job now, select the **Run Now** checkbox. The job will begin running immediately.

  Note Selecting this option ignores any date and time that you enter from the Start Date and Start Time lists.

- To schedule the job for a later date and time, select the month, day, and year from the Start Date lists and select the hour and minutes from the Start Time lists.

Step 3 From the menu in the left pane, go to the next step, Finish. See Finishing the Job, page 4-14.

Downloaded from www.Manualslib.com manuals search engine

Finishing the Job

To validate, save, and add the job to the list of scheduled jobs:

Procedure

Step 1 Click **Finish** in the left pane to complete job creation. The Finish dialog box appears in the right pane. This dialog consists of an Email settings section, a Remote server settings section, a Warnings section and a Validate and Save section.

Step 2 **Email settings section**

If you want email notification of job completion, complete the Email settings section:

Table 4-5 Email Notification Settings for Firmware Jobs

Field	Description
On completion, mail to	Enter a comma-separated list of email addresses to be notified when the job completes.
Email only if job fails	Select this checkbox if you want recipients to be notified only if the job fails.

Tip If email notification is not working, you may need to to set up the mail route by specifying an SMTP server. See Specifying an SMTP Mail Server, page 6-71.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Remote server settings section

If images will be uploaded from a remote TFTP server (instead of being uploaded from the WLSE), complete the Remote server settings section:

Table 4-6 Remote TFTP Server Settings for Firmware Jobs

Field	Description
Use remote server	Select this checkbox to upload the image from a TFTP server. The remote server must have a tftp server running.
Remote server IP address	Enter the IP address of the TFTP server or select a server from the list of recently used servers. Every time you enter a remote server IP address, the address will be added to the Recently used servers list.
Recently used servers	
Remote server filename	The filename of the firmware image file on a remote server. The image file must reside in the main directory for TFTP access on the server.

Step 4 Warnings section

If warnings are detected for any devices during Validate and Save (Step 5), the job will fail for those devices unless you select the **Ignore Warnings** checkbox. If you prefer not to ignore warnings while the job runs, you can correct the warning conditions instead and then validate again.

Step 5 Validate and Save section

a. Click **Validate** to verify that the job will run successfully. If you missed one or more of the numbered steps in the left pane, error messages are displayed (for example, `Devices not Selected`). Correct these errors and click **Validate** again. The Job Validation Summary window opens. For more formation on this window, see Job Validation Summary Window Details, page 4-17.

Note It is recommended that you always validate a job before saving it. Also, you should check the image release notes on Cisco.com for the latest caveat information on the image.

Downloaded from www.Manualslib.com manuals search engine

Note If any fields in the Job Validation Summary window are marked *Error*, the job will fail for those devices unless you correct the error situation.

b. Click **Save** to add the job to the list of scheduled jobs. The screen refreshes and the Job Save Summary window appears, showing the following information:

Table 4-7 Job Save Summary Window

Field	Description
Name	Name of the job.
Description	Job description, if any.
Image	Name of the image selected for the job.
Devices	Names of the devices selected for the job.
Groups	Names of groups selected for the job.
Schedule	Scheduled date and time for the job, or *No Schedule* if the job has not been scheduled.

Step 6 To view the status of the job, select **Firmware > Jobs**. For more information, see Viewing Jobs by Job State, page 4-19.

Related Topics

- Deleting a Job, page 4-22
- Viewing Jobs by Job State, page 4-19
- Viewing Job Run Details, page 4-22

Downloaded from www.Manualslib.com manuals search engine

Job Validation Summary Window Details

The Job Validation Summary window shows the following information:

Table 4-8 Job Validation Summary Window

Field	Description
Image Selected, Version, and Device Type	The image name, image version, and device type that you selected when creating the job.
Image version validation	Whether the image version is valid.
Image known bugs validation	Whether there are any major caveats for this image.
Job protocol validation	Whether the job protocol (HTTP or SNMP) you selected is supported on this device. **Note** Firmware update via SNMP is supported for firmware versions 11.08T and later.
Device-Image validation	Whether the image you selected is valid for this device. This field is marked *Error* if the image is not valid for the type of device you selected.

The Job Validation Summary fields are marked as follows:

- *Passed*—No problems were found.
- *Information*—No problems were found, but there is information you might want to know. For example, the image version you selected is already installed on the device.
- *Warning*—The operation is permitted but may not be advisable; for example, downgrading to an earlier image.

  The selected image will not be applied to devices that have warnings associated with them, unless you deal with the warnings before saving the job. Use one of the following methods to deal with the warnings:

  – Edit your job choices to fix the problems that caused the warnings.

Downloaded from www.Manualslib.com manuals search engine

  - Select the **Ignore Warnings** checkbox in the Warnings section of the Finish dialog box. By default, warnings are not ignored.

- *Error*—The operation is not permitted. The image will not be applied to devices that have errors associated with them. It is recommended that you eliminate the errors before saving the job. If you save a job with errors, the corresponding devices will be ignored during the job run.

Creating a Firmware Job

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Firmware** > **Jobs**. The Jobs window appears.

Step 2 Enter a name for the job and click **Create Job**.

For guidelines on job names, see Naming Guidelines, page A-1.

Step 3 The window refreshes with the Job Creation menu in the left pane and the Job Name dialog box in the right pane.

Step 4 Select the numbered choices in the left pane to create a job. For information on these choices, see Job Choices, page 4-10.

Using the Job Functions

To view job status, select **Firmware** > **Jobs**. The Jobs window appears. This window allows you to view job status, filter a job, edit a job, view details about a job, and undo a job.

Job data is retained for 30 days by default. To change the retention period, see Managing System Parameters, page 6-73.

Note Your login determines whether you can use these options.

Downloaded from www.Manualslib.com manuals search engine

The topics covered in this section are:

- Viewing Jobs by Job State, page 4-19
- Filtering Jobs, page 4-21
- Editing a Job, page 4-21
- Deleting a Job, page 4-22
- Viewing Job Run Details, page 4-22

Related Topic

Creating a Firmware Job, page 4-18

Viewing Jobs by Job State

Procedure

Step 1 From the Job State list, select the type of job whose status you want to check. The window refreshes and the jobs are displayed.

The information displayed depends on which Job State you selected: Scheduled, Unscheduled, Running, or All:

- Scheduled

Field	Description
Job Name	The job name.
Next Schedule	For scheduled jobs, this indicates when the job will run. For completed jobs, this is the time the job ran.
Last Run Status	The status of the last run.

- Unscheduled

Field	Description
Job Name	The job name.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Next Schedule	For scheduled jobs, this indicates when the job will run. For completed jobs, this is the time the job ran.
Last Run Status	The status of the last run.

- Running

Field	Description
Job Name	The job name.
Job Start Time	The time the job started.
Percent Complete	The percent of the job that has completed running.
Next Schedule	Firmware jobs are not recurring.

- All

Field	Description
Job Name	The job name.
Job State	The state of the job. **Note** A job in the DidNotStart state must be rescheduled.
Next Schedule	For scheduled jobs, this indicates when the job will run. For completed jobs, this is when the job ran.
Last Run Status	The status of the job the last time it ran.

Step 2 To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 3 You can do any of the following:

- Filter the job—See Filtering Jobs, page 4-21.
- Edit the job—See Editing a Job, page 4-21.

Downloaded from www.Manualslib.com manuals search engine

- Delete the job—See Deleting a Job, page 4-22.
- View job run details—See Viewing Job Run Details, page 4-22.
- Refresh the screen—Click **Refresh**.

Filtering Jobs

Use this option to display a limited set of jobs, making it easier to search for a particular job by name.

Procedure

Step 1 Click **Filter Job.** The Filter Job dialog box appears.

Step 2 Enter the name, or part of the name. You can use % as a wildcard: for example, entering %name% displays all the jobs that contain the word “name.'

Step 3 Click **Apply filter.** The Job window refreshes and the matching jobs are displayed in the Jobs list.

Note The filter remains in effect until the page is refreshed.

Editing a Job

Use this option to edit jobs from the displayed list of jobs.

Procedure

Step 1 From the list of jobs, select the job that you want to edit.

Step 2 Click **Edit.** The Job Name dialog box appears.

Step 3 Select choices in the Job Creation Menu. For descriptions of the choices, see Job Choices, page 4-10.

Downloaded from www.Manualslib.com manuals search engine

Deleting a Job

Use this option to delete jobs from the displayed list of jobs. Jobs that are scheduled, unscheduled, completed, or did not start can be deleted. Jobs that are running cannot be deleted.

Procedure

Step 1 From the list of jobs, select the job that you want to delete.

Step 2 Click **Delete.**

Step 3 Click **OK** in the popup windows.

Viewing Job Run Details

Use this option to view details about a job.

Procedure

Step 1 From the All Jobs table displayed in the **Firmware > Jobs** window, select a job, then click **Job Run Detail**.

Step 2 The details window appears with the Job Runs table:

Field	Description
Select Run	Used to select a job to see its details.
Job Start Time	The time the job started.
Job End Time	The time the job ended.
Job Status	The status of the job.
Percent Complete	The percent of the job that completed.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Do any of the following:

- To view details for a particular job run, select the job, then click **Show Run Details**. The Job Run details table appears. For more information on this table, see Job Run Details Table, page 4-23.)
- To view the job run log, click **Job Run Log**. A window displays all the details for the selected job number.
- To refresh the table, click **Refresh**.

Job Run Details Table

The Job Runs Details table displays the following information:

Field	Description
Device Name	The name of the device.
Start Time	The time the job started.
End Time	The time the job ended.
Status	The status of the job.

To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Using Reports

The Reports tab displays information about your devices. You can save and email reports. You can also set specific times for emailed reports to be run and sent automatically.

The reports available are dependent on the groups of devices and individual devices you choose from the selector in the left pane.

Following are the subtabs under Reports:

Note Some of the subtabs may not be visible to some users.

- **Device Center**—See Using the Device Center, page 5-1
- **Wireless Clients**—See Displaying Wireless Client Reports, page 5-6
- **Current**—See Displaying Current Reports, page 5-11
- **Trends**—See Displaying Trends, page 5-50
- **Scheduled Email Jobs**—See Scheduling Email Jobs, page 5-68

Using the Device Center

The device center enables you to quickly access various types of reports for a particular device.

Note Your login determines whether you can use this option.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Reports** > **Device Center.** The Device Center appears above the device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 Select the device from the folder in the left pane, and the right pane displays the Summary Report for the device.

Step 4 Click on the buttons for different report types:

- For access points and bridges:
  - Summary report—See Displaying an AP Summary Report, page 5-24
  - Detailed report—See Displaying a Detailed Report, page 5-26
  - Fault Status—See Viewing the Fault Summary Report, page 5-3
  - Device History—See Viewing Device History, page 5-4
  - Config History—See Viewing Config History, page 5-4
  - Firmware History—See Viewing Firmware History, page 5-5
  - AP Web Page—Opens up a browser window to the AP Summary Status.
- For switches:
  - Summary report —SeeDisplaying a Switch Summary Report, page 5-45
  - Fault Status—See Viewing the Fault Summary Report, page 5-3
  - Device History—See Viewing Device History, page 5-4
- For routers:
  - Summary Report—See Displaying a Router Summary Report, page 5-47
  - Fault Status—See Viewing the Fault Summary Report, page 5-3
  - Device History—See Viewing Device History, page 5-4
- For servers—See Displaying a Server Response Time Graph, page 5-65.

Downloaded from www.Manualslib.com manuals search engine

Viewing the Fault Summary Report

The following table is displayed for the device's fault summary:

Table 5-1 Device Fault Summary

Column	Description
Type	The fault type.
Description	A description of the fault. Click to see fault details. See Viewing Fault Details, page 2-5.
Severity	The fault severity level.
State	The current state of the fault.
Timestamp	The time the fault was reported. Click to see fault details. See Viewing Fault Details, page 2-5. For more information, see Time Display, page 1-5.

To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Downloaded from www.Manualslib.com manuals search engine

Viewing Device History

The following table is displayed for the device's history:

Table 5-2 Device History

Column	Description
Timestamp	The time the device's state last changed. For more information, see Time Display, page 1-5.
Device Name	The name of the device.
IP Address	The IP address of the device.
State	The current state of the device.

To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Viewing Config History

The following table is displayed for the device's configuration history:

Table 5-3 Device Configuration History

Column	Description
Start Time	The start time for the device's configuration.
End Time	The end time for the device's configuration.
Job Status	The state of the configuration job.
Template Name	The name of the configuration template used.
Job Protocol	The protocol used for the configuration job.

Downloaded from www.Manualslib.com manuals search engine

Table 5-3 Device Configuration History (continued)

Column	Description
Job Name	The name of the configuration job.
Job Type	The type of configuration job.

To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Viewing Firmware History

The following table is displayed for the device's firmware history:

Table 5-4 Device Firmware History

Column	Description
Start Time	The start time for the device's firmware upgrade job.
End Time	The end time for the device's firmware upgrade job.
Job Status	The state of the firmware job.
Image Name	The name of the firmware image.
Image Version	The version of the firmware.
Image Device Type	The device type.
Job Protocol	The protocol used for the firmware job.
Job Name	The name of the firmware job.

Downloaded from www.Manualslib.com manuals search engine

To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Displaying Wireless Client Reports

Wireless client reports provide information about the type of client that is associating with an access point, information about how much bandwidth the client is using, and a history of which access points the client has been associated with.

Using this window, you can search for a wireless client based on its MAC address or name.

The frequency with which the Wireless Clients reports are updated is 5 minutes by default. To change the default setting, see Managing System Parameters, page 6-73.

Note Your login determines whether you can use this option.

Following are the report types you can view:

- Client Detail Report—See Displaying a Client Detail Report, page 5-6
- Client Statistics Report—See Displaying a Client Statistics Report, page 5-8
- Client Historical Association Report—See Displaying a Client Historical Association Report, page 5-9

Displaying a Client Detail Report

Procedure

Step 1 Select **Reports** > **Wireless Clients**. The Wireless Clients selector appears in the left pane.

Downloaded from www.Manualslib.com manuals search engine

Step 2 From the list, select the method you want to use to search for clients: by MAC address or name.

Step 3 Enter the MAC address or name. You can use an asterisk (*) as a wildcard to denote numbers and letters.

Note The MAC address must be entered in hexadecimal, for example 0070eb37c90.

Step 4 Click **Search**. A list appears in the left pane.

If you chose MAC address in the previous step, MAC addresses are listed; if you chose name, names are listed.

Step 5 Click the MAC address or name. The right pane refreshes and displays the Client Detail Report, which is the default report, with the following information:

Table 5-5 Client Detail Report

Column	Description
Name	The name assigned to the wireless client device.
IP Address	The IP address of the wireless client device.
Classification	The type of wireless client device.
Associated with	The name or IP of the access point with which it was last associated.
State	The operational state of the wireless client device.
Time last seen	The time the client was last seen by the system.
Software Version	The version of wireless client software.
MAC Address	The MAC address of the wireless client.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Downloaded from www.Manualslib.com manuals search engine

Displaying a Client Statistics Report

Procedure

Step 1 Select **Reports** > **Wireless Clients**. The Wireless Clients selector appears in the left pane.

Step 2 From the list, select the method you want to use to search for clients: by MAC address or name.

Step 3 Enter the MAC address or name. You can use an asterisk (*) as a wildcard to denote numbers and letters.

Step 4 Click **Search**. A list appears in the left pane.

Step 5 Select the MAC address or name. The right pane refreshes.

Step 6 From the Report Name list, select **Client Statistics Report**.

Step 7 Click **View**. The Client Statistics Report displays in the right pane with the following information:

Table 5-6 Client Statistics Report

Column	Description
Name	The name of the wireless client.
IP address	The IP address of the wireless client.
Time last seen	The time the wireless client was last seen by the system.
Packets transmitted	The number of packets transmitted.
Octets transmitted	The number of octets transmitted.
Packets received	The number of packets received.
Octets received	The number of octets received.
Latest received signal strength	A tally of the received signal quality.
Latest signal quality	The current index of radio signal quality.
Sleep time in power save mode	The number of beacon intervals across which the station will sleep in power-save mode, or 1 if the station will never be in power-save mode.

Downloaded from www.Manualslib.com manuals search engine

Table 5-6 Client Statistics Report (continued)

Column	Description
Preferred transmission rate	The preferred data transmission rate.
Short retries	The number of times the RTS (request to send) packet had to be retried.
Latest short retries	A tally of the number of retries.
Long retries	The number of times the data packet had to be retried.
Latest long retries	A tally of the number of retries.
Received WEP errors	The number of received encryption errors.
Errors in transmitted packets	The number of errors in transmitted packets.
Errors in received packets	The number of errors in received packets.
Errors in received octets	The number of errors in received octets.
Announcements sent	The total number of announcement packets sent since the device was reset.

Step 8 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 9 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Client Historical Association Report

Procedure

Step 1 Select **Reports** > **Wireless Clients**. The Wireless Clients selector appears in the left pane.

Step 2 From the list, select the method you want to use to search for clients: by MAC address or name.

Step 3 Enter the MAC address or name. You can use an asterisk (*) as a wildcard to denote numbers and letters.

Step 4 Click **Search**. A list appears in the left pane.

Downloaded from www.Manualslib.com manuals search engine

Step 5 Select the MAC address or name. The right pane refreshes.

Step 6 From the Report Name list, select **Client Historical Association Report**.

Step 7 Click **View**. The Client Historical Association Report displays in the right pane with the following information:

Table 5-7 Client Historical Association Report

Column	Description
Associated with	The name or IP address of the AP. Click on this link to view the AP Summary Report and the Fault Summary. For more information, see Displaying an AP Summary Report, page 5-24.
Client IP Address	The IP address of the wireless client device.
Software Version	The software version of the wireless client device.
Associated Time	The time when the WLSE has polled the access point to retrieve the client association time. **Tip** To ensure that you are viewing the most up-to-date information, verify when the last inventory cycle occurred. Client inventory status can be seen by selecting **Administration > Discover > Tasks History > Inventory**.

Step 8 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 9 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 10 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Downloaded from www.Manualslib.com manuals search engine

Displaying Current Reports

This window allows you to view current information about the monitored devices in your network. You can view, export, and email the reports.

The frequency with which configuration data is collected from the devices is 15 minutes by default. To change the default setting, see Managing System Parameters, page 6-73.

Note Your login determines whether you can use this option.

Using this option, you can view the following types of current reports:

- Group Reports, page 5-11
- Individual Access Point and Bridge Reports, page 5-11
- Individual Switch Reports, page 5-12
- Individual Router Reports, page 5-12
- Individual Server Reports, page 5-12

Group Reports

- Group Report—See Displaying a Group Report, page 5-12
- Group Security Report—See Displaying a Group Security Report, page 5-14
- Group SSID Report—See Displaying a Group SSID Report, page 5-16
- Group VLAN Report—See Displaying a Group VLAN Report, page 5-18
- Per VLAN Client Report—See Displaying a Per VLAN Client Report, page 5-20
- Group Policy Report—See Displaying a Group Policy Report, page 5-21

Individual Access Point and Bridge Reports

- Summary Report—See Displaying an AP Summary Report, page 5-24
- Detailed Report—See Displaying a Detailed Report, page 5-26
- Current Client Association—See Displaying a Current Client Association Report, page 5-29

Downloaded from www.Manualslib.com manuals search engine

- EAP Authentication Report—See Displaying an EAP Authentication Report, page 5-30
- AP Ethertype Protocol Filters—See Displaying an AP Ethertype Protocol Filters Report, page 5-32
- AP IP Protocol Filters—See Displaying an AP IP Protocol Filters Report, page 5-33
- AP IP Port Filters—See Displaying an AP IP Port Filters Report, page 5-35
- AP Policy Report—See Displaying an AP Policy Report, page 5-36
- AP QBSS QoS Report—Displaying an AP QBSS QoS Report, page 5-38
- AP SSID Report—Displaying an AP SSID Report, page 5-40
- AP VLAN Report—Displaying an AP VLAN Report, page 5-42
- Per VLAN Client Report—Displaying a Per VLAN Client Report, page 5-43

Individual Switch Reports

- Switch Summary Report—See Displaying a Switch Summary Report, page 5-45
- AP and Bridge Connected to Switch Report—See Displaying an AP and Bridge Connected to Switch Report, page 5-46

Individual Router Reports

- Router Summary Report—See Displaying a Router Summary Report, page 5-47
- AP and Bridge Connected to Router Report—See Displaying an AP and Bridge Connected to Router Report, page 5-48

Individual Server Reports

- Server Summary Report—See Displaying a Server Summary Report, page 5-49

Displaying a Group Report

This report lists all the currently connected access points and bridges in a given group and the total number of clients connected to them. It shows the last polled values and the overall status for the group.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the folder for the group reports you want to view. The right pane refreshes.

Step 3 From the Report Name list, select **Group Report**.

Step 4 Click **View**. The group report is displayed with the following headings:

Table 5-8 Group Report

Column	Description
Number of Clients Associated to this Group	The total number of clients currently associated with the group of access points or bridges.
Count of Active Stations in this Group	The number of access points or bridges currently in the group.
As Of	The time the state of the group last changed. For more information, see Time Display, page 1-5.
AP Name	The name of the access point. Click to view the following: • AP Detailed Report—See Displaying a Detailed Report, page 5-26. • Fault Summary—See Viewing the Fault Summary Report, page 5-3. • EAP Authentication Report—See Displaying an EAP Authentication Report, page 5-30.
AP IP Address	The IP address of the access point. Click to open up a browser window to the AP Summary Status.

Downloaded from www.Manualslib.com manuals search engine

Table 5-8 Group Report (continued)

Column	Description
Number of Clients Connected	The number of wireless clients connected to the device.
Number of Bridges Connected	The number of bridges connected to the access point.
Number of AP-Repeaters Connected	The number of repeaters connected to the access point.
Status (Fault)	Click to view the Fault Summary. For more information, see Viewing the Fault Summary Report, page 5-3.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.

Step 5 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Group Security Report

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Downloaded from www.Manualslib.com manuals search engine

Step 2 From the device selector in the left pane, click to expand the folder for the group security reports you want to view.

Step 3 From the Report Name list, select **Group Security Report**.

Step 4 Click **View**. The group report is displayed with the following headings:

Table 5-9 Group Security Report

Column	Description
AP Name	The name of the device. Click to view the following: • AP Detailed Report—Displaying a Detailed Report, page 5-26. • Fault Summary—Viewing the Fault Summary Report, page 5-3. • EAP Authentication Report—Displaying an EAP Authentication Report, page 5-30.
AP IP Address	The IP address of the device. Click to open up a browser window to the AP Summary Status.
RF Interface	The radio frequency interface.
Encryption type	Indicates the type of encryption used: No Encryption, Optional, or Full Encryption.
Length of WEP Key1 through 4 (in bits)	The WEP key length.
Authentication Type - Open System	Indicates whether any device, regardless of its WEP keys, can authenticate and attempt to associate.
Authentication Type - Shared Key	Indicates whether an access point sends a query to any device attempting to associate with the access point.
Status (Fault)	Click to view the Fault Summary. For more information, see Viewing the Fault Summary Report, page 5-3.

Downloaded from www.Manualslib.com manuals search engine

Table 5-9 Group Security Report (continued)

Column	Description
Link to EAP Authentication Report	Click to view the EAP Authentication report. For more information, see Displaying an EAP Authentication Report, page 5-30.
As Of	The time the fault was reported. For more information, see Time Display, page 1-5.

Step 5 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Group SSID Report

This report displays all the configured SSIDs (both primary and auxiliary) and their corresponding properties in all the devices in the group.

Procedure

Step 1 Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.

Step 2 From the Report Name list, select **Group SSID Report**.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Click **View**. The following report displays the following:

Table 5-10 Group SSID Report

Column	Description
SSID	The unique identifier the client device uses to associate with the access point.
VLAN ID	The identification number of the VLAN.
VLAN Name	The name of the VLAN.
AP Name	The name of the access point. Click to view the following: • AP Detailed Report—See Displaying a Detailed Report, page 5-26. • Fault Summary—See Viewing the Fault Summary Report, page 5-3. • EAP Authentication Report—See Displaying an EAP Authentication Report, page 5-30.
AP IP Address	The IP address of the access point. Click to open up a browser window to the AP Summary Status.
Number of Clients Connected	The number of wireless clients connected to the device.
Priority	The priority configuration based on the traffic type.
Default Policy Group	The number of the default policy group (which contains access parameters). Click to view the Policy Report—See Displaying a Group Policy Report, page 5-21.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.

Downloaded from www.Manualslib.com manuals search engine

Step 4 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 5 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 6 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Group VLAN Report

This report displays all the configured VLANs and their corresponding properties in the group.

Procedure

Step 1 Select **Reports > Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.

Step 2 From the Report Name list, select **Group VLAN Report**.

Step 3 Click **View**. The following report displays the following:

Table 5-11 Group VLAN Report

Column	Description
VLAN ID	The identification number of the VLAN.
VLAN Name	The name of the VLAN.

Downloaded from www.Manualslib.com manuals search engine

Table 5-11 Group VLAN Report (continued)

Column	Description
AP Name	The name of the access point. Click to view the following: • AP Detailed Report—See Displaying a Detailed Report, page 5-26. • Fault Summary—See Viewing the Fault Summary Report, page 5-3. • EAP Authentication Report—See Displaying an EAP Authentication Report, page 5-30.
AP IP Address	The IP address of the access point. Click to open up a browser window to the AP Summary Status.
SSID	The unique identifier the client device uses to associate with the access point.
Number of Clients Connected	The number of wireless clients connected to the device.
Priority	The priority configuration based on the traffic type.
Default Policy Group	The number of the default policy group (which contains access parameters). Click to view the Policy Report—See Displaying a Group Policy Report, page 5-21.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.

Step 4 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Downloaded from www.Manualslib.com manuals search engine

Step 5 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 6 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Per VLAN Client Report

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.

Step 2 From the Report Name list, select **Per VLAN Client Report**.

Step 3 Click **View**. The following report displays the following:

Table 5-12 Per VLAN Client Report

Column	Description
VLAN ID	The identification number of the VLAN.
VLAN Name	The name of the VLAN.
AP Name	The name of the access point. Click to view the following: • AP Detailed Report—See Displaying a Detailed Report, page 5-26. • Fault Summary—See Viewing the Fault Summary Report, page 5-3. • EAP Authentication Report—See Displaying an EAP Authentication Report, page 5-30.
Client MAC Address	The MAC address of the client.
Client Name	The name of the client.
Client IP Address	The IP address of the client.
SSID	The unique identifier the client device uses to associate with the access point.

Downloaded from www.Manualslib.com manuals search engine

Table 5-12 Per VLAN Client Report (continued)

Column	Description
Client Type	The type of client.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.

Step 4 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 5 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 6 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Group Policy Report

This report lists all the policy groups configured on each of the access points in this group.

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane. From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.

Step 2 From the Report Name list, select **Group Policy Report**.

Downloaded from www.Manualslib.com manuals search engine

Step 3 Click **View**. The following report displays the following:

Table 5-13 Group Policy Report

Column	Description
AP Name	The name of the access point. Click to view the following: • AP Detailed Report—See Displaying a Detailed Report, page 5-26. • Fault Summary—See Viewing the Fault Summary Report, page 5-3. • EAP Authentication Report—See Displaying an EAP Authentication Report, page 5-30.
AP IP Address	The IP address of the access point. Click to open up a browser window to the AP Summary Status.
Policy Group Id	The identification number of the policy group.
Policy Group Name	The name of the policy group.
Ethertype Filter Id (In)	The identification number of the (receive) Ethertype filter. Click to view the AP Ethertype Protocol Filters Report—See Displaying an AP Ethertype Protocol Filters Report, page 5-32.
Ethertype Filter Id (Out)	The identification number of the (transmit) Ethertype filter. Click to view the AP Ethertype Protocol Filters Report—See Displaying an AP Ethertype Protocol Filters Report, page 5-32.
IP Protocol Filter Id (In)	The identification number of the (receive) IP protocol filter. Click to view the AP IP Protocol Filters Report—See Displaying an AP IP Protocol Filters Report, page 5-33.

Downloaded from www.Manualslib.com manuals search engine

Table 5-13 Group Policy Report (continued)

Column	Description
IP Protocol Filter Id (Out)	The identification number of the (transmit) IP protocol filter Click to view the AP IP Protocol Filters Report—See Displaying an AP IP Protocol Filters Report, page 5-33.
IP Port Filter Id (In)	The identification number of the (receive) IP port filter. Click to view the AP IP Port Filters Report—See Displaying an AP IP Port Filters Report, page 5-35.
IP Port Filter Id (Out)	The identification number of the (transmit) IP port filter. Click to view the AP IP Port Filters Report—See Displaying an AP IP Port Filters Report, page 5-35.
As Of	The time the device's state last changed. For more information, see Time Display, page 1-5.

Step 4 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 5 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 6 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Downloaded from www.Manualslib.com manuals search engine

Displaying an AP Summary Report

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the device for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **Summary Report**.

Step 5 Click **View**. Two tables are displayed: the AP Summary Report and the Fault Summary.

Note If the selected device has dual interfaces, two summary reports are displayed, one for each interface.

Table 5-14 AP Summary Report

Column	Description
Name	The system name for the device.
As Of	The time the device's state last changed. For more information, see Time Display, page 1-5.
MAC Address	The device's MAC address.

Downloaded from www.Manualslib.com manuals search engine

Table 5-14 AP Summary Report (continued)

Column	Description
IP Address	The device's IP address. Click to open up a browser window to the AP Summary Status.
Software Version	The version of software running on the device.
Number of Clients connected	The number of wireless clients connected to the device.
Number of Bridges Connected	The number of wireless bridges connected to the device.
Number of AP-Repeaters Connected	The number of AP repeaters connected to the device.
Model	Model number of the device.
SSID	The unique identifier the client device uses to associate with the access point.
Radio Cell Role	Indicates whether the device is used as a root or repeater.
Link to the Detailed Report	Click to see details. For more information, see Displaying a Detailed Report, page 5-26.
Link to the Association Report	Click to see associations. For more information, see Displaying a Current Client Association Report, page 5-29.
Link to the Access Point Web Page	Click to open up a browser window to the AP Summary Status.

For information on the Fault Summary, see Viewing Fault Details, page 2-5.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Downloaded from www.Manualslib.com manuals search engine

Displaying a Detailed Report

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the device for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **Detailed Report**.

Step 5 Click **View**. In addition to the Detailed Report, the Fault Summary, and the EAP Authentication Report are also displayed.

Note If the selected device has dual interfaces, two summary reports are displayed, one for each interface.

Table 5-15 Detailed Report

Column	Description
System Name	The system name for the device.
As Of	The time the device's state last changed. For more information, see Time Display, page 1-5.
MAC Address	The device's MAC address.

Downloaded from www.Manualslib.com manuals search engine

Table 5-15 Detailed Report (continued)

Column	Description
IP Address	The device's IP address. Click to open up a browser window to the AP Summary Status.
Software Version	The device's software version.
Number of Clients Connected	The number of wireless clients connected to the device.
Number of Bridges Connected	The number of bridges connected to the device.
Number of AP-Repeaters Connected	The number of AP repeaters connected to the device.
Model	The hardware model of the device.
SSID	The unique identifier the client device uses to associate with the access point.
Radio Cell Role	Indicates the role of the device.
Subnet Mask	The subnet mask.
Ensure Compatibility With 2Mbps Clients	Indicates whether it is compatible with 2Mbps clients.
Ensure Compatibility With non-Aironet 802.11	Indicates whether it is compatible with 802.11.
SNMP Trap Destination	The IP address or host name of the server running the SNMP Management software.
HTTP Port	The device's HTTP setting.
Hot StandBy	Indicates whether the hot standby unit is in monitoring mode. If true, the current unit is in monitoring mode.
Count of Access Point observed by this AP	Number of access points seen by the access points.
Current operating frequency channel	The radio channel being used.

Downloaded from www.Manualslib.com manuals search engine

Table 5-15 Detailed Report (continued)

Column	Description
Ethernet Port Status	The operational status of the Ethernet port.
Radio Port Status	The operational status of the radio port.
Transmit Power (mW)	The access point's transmission power setting in milliwatts.
Switch IP (to which this AP is attached)	The IP address of the switch to which this access point is attached.
Switch Name (to which this AP is attached)	The name of the switch to which this access point is attached.
Encryption type	Indicates that devices using WEP are allowed to communicate with the access point.
Length of WEP key 1 through 4 (in bits)	The WEP key length.
Authentication Type - Open System	Indicates whether any device, regardless of its WEP keys, can authenticate and attempt to associate.
Authentication Type - Shared Key	Indicates whether an access point sends a query to any device attempting to associate with the access point.
Link to the Access Point Web Page	Click to open up a browser window to the AP Summary Status.

- For Fault Summary information, see Viewing Fault Details, page 2-5.
- For EAP Authentication Report, see Displaying an EAP Authentication Report, page 5-30.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Downloaded from www.Manualslib.com manuals search engine

Displaying a Current Client Association Report

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the access point for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **Current Client Association Report**.

Downloaded from www.Manualslib.com manuals search engine

Step 5 Click **View**. The group report is displayed with the following headings:

Table 5-16 Current Client Association Report

Column	Description
Name	The name of the client associated with the access point.
IP Address	The IP address of the wireless client.
MAC Address	The wireless client's MAC address.
Device Type	The wireless client device type.
As Of	The time the device was last seen by the system. For more information, see Time Display, page 1-5.
State	The operational state of the device.

Step 6 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying an EAP Authentication Report

This device report lists all the authentication servers that are configured for the access point.

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Downloaded from www.Manualslib.com manuals search engine

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the access point for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **EAP Authentication Report**.

Step 5 Click **View**. The report is displayed with the following headings:

Table 5-17 EAP Authentication Report

Column	Description
Server Name	The name of the authentication server.
Server Protocol	The protocol used by the server.
Server Priority	The priority of the server when multiple servers are configured for the same service.
Server Port	The communication port setting used by the access point and the server.

Downloaded from www.Manualslib.com manuals search engine

Step 6 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying an AP Ethertype Protocol Filters Report

This device report lists the Ethertype protocol filters configured on the access point.

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the access point for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **AP Ethertype Protocol Filters**.

Downloaded from www.Manualslib.com manuals search engine

Step 5 Click **View**. The report is displayed with the following headings:

Table 5-18 AP Ethertype Protocol Filters Report

Column	Description
Filter Set Id	The identification number of the filter set.
Filter Set Name	The name of the filter set.
Default Disposition	The type of disposition configured: Forward (to forward protocol traffic, or Block (to block protocol traffic).
Filter Special Case Ethertype	The special case configuration.
Filter Special Case Disposition	The special case disposition.
Filter Special Case Priority	The priority configuration based on the traffic type.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.

Step 6 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying an AP IP Protocol Filters Report

This device report lists the IP protocol filters configured on the access point.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the access point for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **AP IP Protocol Filters**.

Step 5 Click **View**. The report is displayed with the following headings:

Table 5-19 AP IP Protocol Filters Report

Column	Description
Filter Set Id	The identification number of the filter set.
Filter Set Name	The name of the filter set.
Default Disposition	The type of disposition configured: Forward (to forward protocol traffic, or Block (to block protocol traffic).
Filter Special Case IP Protocol	The special case configuration.
Filter Special Case Disposition	The special case disposition.
Filter Special Case Priority	The priority configuration based on the traffic type.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.

Downloaded from www.Manualslib.com manuals search engine

Step 6 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying an AP IP Port Filters Report

This device report lists the various IP port filters configured on the access point.

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the access point for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **AP IP Port Filters**.

Downloaded from www.Manualslib.com manuals search engine

Step 5 Click **View**. The report is displayed with the following headings:

Table 5-20 AP IP Port Filters Report

Column	Description
Filter Set Id	The identification number of the filter set.
Filter Set Name	The name of the filter set.
Default Disposition	The type of disposition configured: Forward (to forward protocol traffic, or Block (to block protocol traffic).
Filter Special Case IP Port	The special case configuration.
Filter Special Case Disposition	The special case disposition.
Filter Special Case Priority	The priority configuration based on the traffic type.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.

Step 6 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying an AP Policy Report

This device report lists all the policy groups configured on the access point.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the access point for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **AP Policy Report**.

Step 5 Click **View**. The report is displayed with the following headings:

Table 5-21 AP Policy Report

Column	Description
Policy Group Id	The identification number for the policy group.
Policy Group Name	The name of the policy group.
Ethertype Filter Id (In)	The identification number of the (receive) Ethertype filter. Click to see the AP Ethertype Protocol Filters Report—See Displaying an AP Ethertype Protocol Filters Report, page 5-32.
Ethertype Filter Id (Out)	The identification number of the (transmit) Ethertype filter. Click to see the AP Ethertype Protocol Filters Report—See Displaying an AP Ethertype Protocol Filters Report, page 5-32.
IP Protocol Filter Id (In)	The identification number of the (receive) IP protocol filter. Click to see the AP Ethertype Protocol Filters Report—See Displaying an AP IP Protocol Filters Report, page 5-33.

Downloaded from www.Manualslib.com manuals search engine

Table 5-21 AP Policy Report (continued)

Column	Description
IP Protocol Filter (Out)	The identification number of the (transmit) IP protocol filter. Click to see the AP IP Protocol Filters Report—See Displaying an AP IP Protocol Filters Report, page 5-33.
IP Port Filter Id (In)	The identification number of the (receive) IP port filter. Click to see the AP IP Port Filters Report—See Displaying an AP IP Port Filters Report, page 5-35.
IP Port Filter Id (Out)	The identification number of the (transmit) IP port filter. Click to see the AP IP Port Filters Report—See Displaying an AP IP Port Filters Report, page 5-35.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.

Step 6 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying an AP QBSS QoS Report

This device report displays the configured QoS parameters and whether QBSS is enabled or disabled.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the access point for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **AP QBSS QoS Report**.

Step 5 Click **View**. The report is displayed with the following headings:

Table 5-22 AP QBSS QoS Report

Column	Description
RF Interface	The radio frequency interface.
Traffic Category	The category of traffic.
CWmin	The minimum contention window value.
CWmax	The maximum contention window value.
Generate QBSS Element	Indicates if basic 802.11 quality of service is enabled or disabled.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.

Step 6 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Downloaded from www.Manualslib.com manuals search engine

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying an AP SSID Report

This device report displays all the configured SSIDs (both primary and auxiliary) and their corresponding properties.

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the access point for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **AP SSID Report**.

Step 5 Click **View**. The report is displayed with the following headings:

Table 5-23 AP SSID Report

Column	Description
SSID	The unique identifier the client device uses to associate with the access point.
VLAN ID	The VLAN identification number.
VLAN Name	The VLAN name.

Downloaded from www.Manualslib.com manuals search engine

Table 5-23 AP SSID Report (continued)

Column	Description
Number of Clients Connected	The number of wireless clients connected to the device.
Priority	The priority configuration based on the traffic type.
Default Policy Group	The number of the default policy group (which contains access parameters). Click to view the AP Policy Report—See Displaying an AP Policy Report, page 5-36.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.

Downloaded from www.Manualslib.com manuals search engine

Step 6 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying an AP VLAN Report

This device report displays all the configured VLANs and their corresponding properties.

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the access point for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **AP VLAN Report**.

Downloaded from www.Manualslib.com manuals search engine

Step 5 Click **View**. The report is displayed with the following headings:

Table 5-24 AP VLAN Report

Column	Description
VLAN ID	The identification number of the VLAN.
VLAN Name	The name of the VLAN.
SSID	The unique identifier the client device uses to associate with the access point.
Number of Clients Connected	The number of wireless clients connected to the device.
Priority	The priority configuration based on the traffic type.
Default Policy Group	The number of the default policy group (which contains access parameters).
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.

Step 6 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Per VLAN Client Report

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Downloaded from www.Manualslib.com manuals search engine

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the access point for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **Per VLAN Client Report**.

Step 5 Click **View**. The report is displayed with the following headings:

Table 5-25 Per VLAN Client Report

Column	Description
VLAN ID	The identification number of the VLAN.
VLAN Name	The name of the VLAN.
Client MAC Address	The MAC address of the client.
Client Name	The name of the client.
Client IP Address	The IP address of the client.
SSID	The unique identifier the client device uses to associate with the access point.
Client Type	The type of client associated to the access point.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.

Step 6 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Downloaded from www.Manualslib.com manuals search engine

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Switch Summary Report

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the switch for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **Switch Summary Report**.

Step 5 Click **View**. The group report is displayed with the following headings:

Table 5-26 Switch Summary Report

Column	Description
System Name	The switch name.
IP Address	The switch IP address or hostname.
System Description	A description of the system.
Location	A description of the switch location.
Product Type	The switch type.

Downloaded from www.Manualslib.com manuals search engine

Table 5-26 Switch Summary Report (continued)

Column	Description
System Version	The software version on the switch.
Link to the AP and Bridge Connected	Click for details. For more information, see Displaying an AP and Bridge Connected to Switch Report, page 5-46.

Step 6 For information on the Fault Summary table, see Viewing the Fault Summary Report, page 5-3

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying an AP and Bridge Connected to Switch Report

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the switch for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **AP and Bridge Connected to Switch Report**.

Downloaded from www.Manualslib.com manuals search engine

Step 5 Click **View**. The report is displayed with the following headings:

Table 5-27 AP and Bridge Connected to Switch Report

Column	Description
Device Port	The device port.
AP Name	The name of the access point or bridge connected to the switch.
AP IP Address	The IP address of the access point or bridge connected to the switch.
Status (Fault)	The fault status. Click for details. For more information, see Viewing the Fault Summary Report, page 5-3.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Router Summary Report

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the router for which you want a report. The right pane refreshes.

Downloaded from www.Manualslib.com manuals search engine

Step 4 From the Report Name list, select **Router Summary Report**.

Step 5 Click **View**. The group report is displayed with the following headings:

Table 5-28 Router Summary Report

Column	Description
System Name	The router name.
IP Address	The router IP address.
System Description	A description of the router.
Location	The location of the router.
Product Type	The router hardware type.
System Version	The router version.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying an AP and Bridge Connected to Router Report

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder and select the switch for which you want a report. The right pane refreshes.

Downloaded from www.Manualslib.com manuals search engine

Step 4 From the Report Name list, select **AP and Bridge Connected to Router Report**.

Step 5 Click **View**. The report is displayed with the following headings:

Table 5-29 AP and Bridge Connected to Router Report

Column	Description
Device Port	The device port.
AP Name	The name of the access point or bridge connected to the router.
AP IP Address	The IP address of the access point or bridge connected to the router.
Status (Fault)	The fault status. Click for details. For more information, see Viewing the Fault Summary Report, page 5-3.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Server Summary Report

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Downloaded from www.Manualslib.com manuals search engine

Step 3 From the device selector in the left pane, click to expand the folder and select the server for which you want a report. The right pane refreshes.

Step 4 From the Report Name list, select **Summary Report** for the server.

Step 5 Click **View**. The report is displayed with the following headings:

Table 5-30 Summary Report

Column	Description
Server Name	The name of the server.
Port	The port number used for authentication.
User Name	The user name used for authentication.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying Trends

This window allows you to view trends about the monitored access points, bridges, and servers in your network. You can view, export, and email the reports.

Note Trending reports are not shown for routers or switches.

The frequency with which performance data is aggregated is 3 hours by default. To change the default setting, see Managing System Parameters, page 6-73.

Note Your login determines whether you can use this option.

Using this option, you can view the following types of trend reports:

- Group Reports
  - Group Performance Report: RF Utilization—Displaying a Group Performance Report: RF Utilization, page 5-51

Downloaded from www.Manualslib.com manuals search engine

  - Group Performance Report: Ethernet Utilization—See Displaying a Group Performance Report: Ethernet Utilization, page 5-53.
  - Top N Number of Associations—See Displaying a Top N Number of Associations Report, page 5-54
  - Top N Percentage Errors—See Displaying a Top N Percentage Errors, page 5-55
- Individual Access Point and Bridge Reports
  - AP and Bridge RF Transmission Statistics—See Displaying an AP and Bridge RF Transmission Statistics Report, page 5-56.
  - AP and Bridge Ethernet Transmission Statistics—See Displaying an AP and Bridge Ethernet Transmission Statistics Report, page 5-58.
  - AP and Bridge Performance: Graph—See Displaying an AP and Bridge Performance Graph, page 5-60.
  - AP and Bridge Performance: Tabular—See Displaying an AP and Bridge Performance: Tabular, page 5-61.
  - Top N Busiest Clients—See Displaying Top N Busiest Clients, page 5-62
  - Top N Client Error Rate—See Displaying Top N Client Error Rate, page 5-64
- Servers

  Server Response Time Graph—See Displaying a Server Response Time Graph, page 5-65.

Displaying a Group Performance Report: RF Utilization

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click the group folder for which you want a report. The right pane refreshes.

Step 3 From the Report Name list, select **Group Performance Report: RF Utilization.**

Downloaded from www.Manualslib.com manuals search engine

Step 4 From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.

Step 5 Click **View**. The table is displayed:

Table 5-31 Group Performance Report: RF Utilization

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.
RF Interface	The radio frequency interface.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.
RF Utilization (%)	The percentage of radio frequency utilization.
Number of Associations	Shows the number of associations with clients.
SSID	The unique identifier the client device uses to associate with the access point.
Channel Number	The channel being used.

Step 6 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Downloaded from www.Manualslib.com manuals search engine

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Group Performance Report: Ethernet Utilization

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.

Step 3 From the Report Name list, select **Group Performance Report: Ethernet Utilization**.

Step 4 From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.

Step 5 Click **View**. The table is displayed:

Table 5-32 Group Performance Report: Ethernet Utilization

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.
Ethernet Utilization (%)	The percentage of Ethernet utilization.
Number of Associations	Shows the number of associations with clients.

Downloaded from www.Manualslib.com manuals search engine

Table 5-32 Group Performance Report: Ethernet Utilization (continued)

Column	Description
SSID	The unique identifier the client device uses to associate with the access point.
Channel Number	The channel being used.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Top N Number of Associations Report

This report lists the top number of access points which have the highest average number of associations over the selected period of time. The minimum and maximum number of associations are also displayed.

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.

Step 3 From the Report Name list, select **Top N Number of Associations**.

Step 4 From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.

Step 5 In the N Value text box, enter the top number of associations you want to view.

Step 6 Click **View**. The table is displayed:

Downloaded from www.Manualslib.com manuals search engine

Table 5-33 Top N Number of Associations

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.
Number of Clients Connected (Avg)	The average number of clients connected to the access point.
Number of Clients Connected (Min)	The minimum number of clients connected to the access point.
Number of Clients Connected (Max)	The maximum number of clients connected to the access point.

Step 7 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 8 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 9 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Top N Percentage Errors

This report lists the top number of access points which have the highest average percentage of errors. The minimum and maximum percentage of errors during the selected period of time are also displayed.

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.

Downloaded from www.Manualslib.com manuals search engine

Step 3 From the Report Name list, select **Top N Percentage Errors**.

Step 4 From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.

Step 5 In the N Value text box, enter the top number of errors you want to view.

Step 6 Click **View**. The table is displayed:

Table 5-34 Top N Percentage Errors

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.
RF Interface	The radio frequency interface.
Packet Errors (Avg) (%)	The average percentage of error packets.
Packet Errors (Min) (%)	The minimum percentage of error packets.
Packet Errors (Max) (%)	The maximum percentage of error packets.

Step 7 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 8 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 9 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying an AP and Bridge RF Transmission Statistics Report

This report displays the transmit and receive rates overlaid in a graph.

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Downloaded from www.Manualslib.com manuals search engine

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder, then select the devices for which you want to see a report. The right pane refreshes.

Step 4 From the Report Name list, select **AP and Bridge RF Transmission Statistics**.

Step 5 From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.

Step 6 Click **View**. A graph is displayed:

Table 5-35 AP and Bridge RF Transmission Statistics

Column	Description
Transmit Rate	The x-axis displays the time intervals. The y-axis displays the number of packets transmitted per second.
Receive Rate	The x-axis displays the time intervals. The y-axis displays the number of packets received per second.
Packet Errors	The x-axis displays the time intervals. The y-axis displays the number of error packets per number of packets.

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Downloaded from www.Manualslib.com manuals search engine

Displaying an AP and Bridge Ethernet Transmission Statistics Report

This report displays the transmit and receive rates overlaid in a graph.

Procedure

Step 1 Select **Reports > Trends**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder, then select the devices for which you want to see a report. The right pane refreshes.

Step 4 From the Report Name list, select **AP and Bridge Ethernet Transmission Statistics**.

Step 5 From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.

Step 6 Click **View**. A graph is displayed:

Table 5-36 AP and Bridge Ethernet Transmission Statistics

Column	Description
Transmit Rate	The x-axis displays the time intervals. The y-axis displays the number of packets transmitted per second.

Downloaded from www.Manualslib.com manuals search engine

Table 5-36 AP and Bridge Ethernet Transmission Statistics (continued)

Column	Description
Receive Rate	The x-axis displays the time intervals. The y-axis displays the number of packets received per second.
Packet Errors	The x-axis displays the time intervals. The y-axis displays the number of error packets per number of packets.

Downloaded from www.Manualslib.com manuals search engine

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying an AP and Bridge Performance Graph

This report displays the Ethernet utilization and RF utilization overlaid in a graph.

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder you want to view. The right pane refreshes.

Step 4 From the Report Name list, select **AP and Bridge Performance Graph**.

Step 5 From the Start Date list, select the start date for the graph, and from the For a period of list, select the number of days.

Downloaded from www.Manualslib.com manuals search engine

Step 6 Click **View**. A graph is displayed:

Table 5-37 AP and Bridge Performance Graph

Column	Description
RF Utilization	The x-axis displays the time intervals. The y-axis displays the percent of radio frequency utilization.
Ethernet Utilization	The x-axis displays the time intervals. The y-axis displays the percent of Ethernet utilization.
Number of Associations	The x-axis displays the time intervals. The y-axis displays the number of client associations

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying an AP and Bridge Performance: Tabular

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Downloaded from www.Manualslib.com manuals search engine

Step 3 From the device selector in the left pane, click to expand the folder you want to view. The right pane refreshes.

Step 4 From the Report Name list, select **AP and Bridge Performance: Tabular**.

Step 5 From the Start Date list, select the start date for the graph, and from the For a period of list, select the number of days.

Step 6 Click **View**. The report is displayed:

Table 5-38 AP and Bridge Performance: Tabular

Column	Description
IP Address	The IP address of the access point or bridge.
As Of	The time the access point's state last changed. For more information, see Time Display, page 1-5.
Number of Associations	The number of client associations.
Ethernet Utilization (%)	The amount of Ethernet utilization.
RF Interface	The radio frequency interface.
RF Utilization (%)	The amount of radio frequency utilization.

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying Top N Busiest Clients

This report lists the top number of busiest clients in terms of average bit rate as perceived by the access point for the selected period of time. The minimum and maximum bit rates for the clients are also displayed.

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Downloaded from www.Manualslib.com manuals search engine

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder you want to view. The right pane refreshes.

Step 4 From the Report Name list, select **Top N Busiest Clients**.

Step 5 From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.

Step 6 In the N Value text box, enter the top number of clients you want to view.

Step 7 Click **View**. The table is displayed:

Table 5-39 Top N Busiest Clients

Column	Description
Client Name	The name of the client.
Client IP Address	The IP address of the client.
Client MAC Address	The MAC address of the client.
Bit Rate (Avg) (in kbps)	The average bit rate for the client.
Bit Rate (Min) (in kbps)	The minimum bit rate for the client.
Bit Rate (Max) (in kbps)	The maximum bit rate for the client.

Step 8 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 9 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 10 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Downloaded from www.Manualslib.com manuals search engine

Displaying Top N Client Error Rate

This report lists the top number of clients in terms of average bit error rate as perceived by the access point for the selected period of time. The minimum and maximum bit error rates for the clients are also displayed.

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder you want to view. The right pane refreshes.From the Report Name list, select **Top N Client Error Rate**.

Step 4 From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.

Step 5 In the N Value text box, enter the top number of clients you want to view.

Step 6 Click **View**. The table is displayed:

Table 5-40 Top N Client Error Rate

Column	Description
Client Name	The name of the client.
Client IP Address	The IP address of the client.
Client MAC Address	The MAC address of the client.
Bit Error Rate (Avg) (in kbps)	The average bit error rate for the client.
Bit Error Rate (Min) (in kbps)	The minimum bit error rate for the client.
Bit Error Rate (Max) (in kbps)	The maximum bit error rate for the client.

Downloaded from www.Manualslib.com manuals search engine

Step 7 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 8 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 9 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Displaying a Server Response Time Graph

This graph plots the response time of the server over the period of time specified.

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 If you want to search for the device, use the dialog box in the left pane above the device selector:

a. From the list, select the method you want to use to search for the device: by name or by IP address.

b. Enter the IP address or name, or use an asterisk (*) as a wildcard to denote numbers and letters, then click **Search**. The requested device appears in the Search Results folder.

Step 3 From the device selector in the left pane, click to expand the folder you want to view. The right pane refreshes.

Step 4 From the Report Name list, select **Server Response Time Graph**.

Step 5 From the Start Date list, select the start date for the graph, and from the For a period of list, select the number of days.

Downloaded from www.Manualslib.com manuals search engine

Step 6 Click **View**. The following report displays:

Table 5-41 Server Response Time Graph

Column	Description
Server Response Time	The x-axis displays the time intervals. The y-axis displays the response time in milliseconds.

Step 7 To export the report, click **Export.** (See Exporting a Report, page 5-66.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 5-66.)

Exporting a Report

Step 1 Click **Export**. An Export window appears.

Step 2 From the Output Format list, select the format in which you want the file exported: CSV, PDF, or XML.

Step 3 Click **Submit**. A window opens in the requested format and displays the output.

Emailing a Report

Procedure

Step 1 Click **Email Report**. A the right pane refreshes with an Email properties dialog box.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Enter the following:

Tip If email notification is not working, you may need to configure the mailroute by selecting **Administration** > **Appliance** > **Configure Mailroute**.

Field	Description
To	Enter the email address of the person to whom you want to send the report. An entry in this field is required.
Cc	Enter email addresses of persons that you want to copy on the email.
Subject	Enter a subject for the email.
Attachment Type	From the list, select the format in which you would like the report sent: CSV, PDF, or XML.
Message	Enter any message you would like to send.
Report Data for Last 'N' Days	This entry is applicable for Trends reports only. From the list, select the number of days for which you want report data emailed.

Step 3 To cancel the email, click **Cancel**.

Step 4 To send the email immediately, click **Send Now**.

Step 5 To schedule the email for later:

a. Click **Schedule**. The schedule job dialog box appears.

b. Enter the following:

Field	Description
Job Name	Enter a name for the job. For more information, see Naming Guidelines, page A-1.
Start Date	From the list, select the date you would like to send the email.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Start Time	From the list, select the time you would like to send the email.
Repeat	
Enable	Check if you want to set up a scheduled job that periodically sends email.
Every	From the list, select the period of time you would like the email sent.

Step 6 Do one of the following:

- Click **Cancel** to cancel the schedule.
- Click **Finish** to complete scheduling. You receive a confirmation message that your email has been scheduled.

Step 7 To view, delete, or edit the scheduled email jobs, see Scheduling Email Jobs, page 5-68

Scheduling Email Jobs

This window allows you to view information about email jobs you have scheduled. It also allows you to delete them and edit them.

The length of time job data is retained is 30 days by default. To change the default setting, see Managing System Parameters, page 6-73.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Reports** > **Scheduled Email Jobs**. The Email Jobs window appears.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Job Name	The name of the job. For more information, see Naming Guidelines, page A-1.
Recurring	Indicates whether it is a recurring job.
Next Schedule	Indicates when the job runs again.

Step 2 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 3 To delete a job, select it, then click **Delete Email Job**.

Step 4 To view an email job, select it, then click **View Email Job**. (See Viewing Email Job Details, page 5-69.)

Step 5 To edit a job, select it, then click **Edit Email Job**. The email appears and allows you to change any of the entries. (See Emailing a Report, page 5-66 for more information.)

Viewing Email Job Details

The following tables are displayed in a window when you select a job in **Reports > Scheduled Email Jobs**, then click **View Email Job**.

Report Properties

Column	Description
User Name	The name of the user who scheduled the job.
Report Type	The report type.
Report Name	The report name.

Downloaded from www.Manualslib.com manuals search engine

Email Properties

Column	Description
To	The username of the person to whom the report is being emailed.
Cc	The username of the person to whom the report is being copied.
Subject	The email subject.
Format	The format in which the report is being emailed.
Body	The text entered into the body of the email.

Schedule Properties

Column	Description
Email Job Name	The name of the email job.
Start Date	The date the report is emailed.
Frequency	The frequency with which the report is to be emailed.

Downloaded from www.Manualslib.com manuals search engine

Performing Administrative Tasks

The Administration tab allows you to you perform administrative tasks.

Note Some of the subtabs may not be visible to some users; what you view under the Administration tab depends on your login.

The Administration subtabs have the following functions:

- **Discover**—Manage devices, configure and run discovery, specify device credentials, run inventory, view discovery and inventory history, import and export devices, and set up AAA servers (see Using Discovery and Managing Devices, page 6-2).
- **Group Management**—Create groups for efficient device management and place devices in them (see Managing Groups, page 6-37).
- **Appliance**—Manage the Wireless LAN Solution Engine server (see Managing the Appliance, page 6-44).
- **System Parameters**—Configure polling parameters for collecting data from devices (see Managing System Parameters, page 6-73).
- **User Admin**—Manage users and user roles (see Administering Users, page 6-75).
- **My Profile**—Change your password (see Modifying Your Profile, page 6-80).
- **Links**—Set up links to CiscoWorks2000 servers and display server desktops (see Linking to a CiscoWorks2000 Server, page 6-81).

Downloaded from www.Manualslib.com manuals search engine

Using Discovery and Managing Devices

When you select **Administration** > **Discover**, the following options appear in the left pane:

- **Managed Devices**—View newly discovered devices, change device status, and view device management history—see Managing Devices, page 6-2.
- **Device Credentials**—Specify community strings for all managed devices and specify the HTTP usernames and passwords for access points (see Specifying Device Credentials, page 6-6).
- **Discover**—Schedule discovery, perform an immediate discovery, set up discovery filters, and set discovery options (including auto-manage—see Managing Device Discovery, page 6-10.
- **Inventory**—Run a one-time, immediate inventory to collect information from managed devices before the next *scheduled* inventory (see Running Inventories, page 6-24)
- **Task History**—View details on discovery and inventory jobs (See Viewing Inventory and Discovery Task History, page 6-27).
- **Import Devices**—Import devices from a file or from a CiscoWorks2000 server (see Importing Devices, page 6-28).
- **Export Devices**—Export devices to a CiscoWorks2000 server (see Exporting Devices, page 6-31).
- **LEAP Server**—Add, modify, and delete LEAP servers (see Adding, Modifying and Deleting AAA Servers, page 6-33).
- **RADIUS Server**—Add, modify, and delete RADIUS servers (see Adding, Modifying and Deleting AAA Servers, page 6-33).
- **EAP-MD5 Server**—Add, modify, and delete EAP-MD5 servers (see Adding, Modifying and Deleting AAA Servers, page 6-33).

Managing Devices

Before you can view discovered devices or perform any operations on them, you must move the devices to the managed state. When you select **Administration** > **Discover** > **Managed Devices**, the following options are displayed:

Downloaded from www.Manualslib.com manuals search engine

- **Manage/Unmanage**—View newly discovered devices, change device management status, or delete devices (see Manage Devices, page 6-3).
- **Device History**—View the management history of each discovered device (see View Device Management History, page 6-5).

Manage Devices

You can use this option to change a device's management status or delete a device.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration** > **Discover** > **Managed Devices** > **Manage/Unmanage**. The device selector is displayed, showing:

- Newly discovered devices (New folder). All new devices are also listed in the Unmanaged folder.
- Managed devices (Managed folder)
- Unmanaged devices (Unmanaged folder).

Step 2 To view the contents of a folder, expand the folder.

Step 3 To modify the status of the devices in a folder, click the folder name. The Group Status pane appears. Select one or more devices from the list and click **Manage** or **Unmanage** in the Group Change Status window. Devices are moved into the Managed or Unmanaged folders.

You must move newly discovered devices to the managed state. Only managed devices appear in WLSE displays.

Tip If you want all discovered devices to be automatically moved to the managed state, enable auto-manage in **Administration** > **Discover** > **DISCOVER** > **Discovery Options**. For more information, see Enable Discovery Options, page 6-18.

Downloaded from www.Manualslib.com manuals search engine

Note You can only manage a total of 525 access points and wireless bridges. After you have placed 500 of these devices into the Managed folder, warning messages are displayed each time you place more devices in the folder. After the 525 limit is reached, no more devices can be placed in the Managed folder, although discovery continues after the limit is reached.

Step 4 After you move devices to the managed state, inventory is run for those devices. This ensures that device attributes appear in displays, such as reports and system-defined groups without waiting for the next inventory cycle. For information about running an immediate inventory, see Running Inventories, page 6-24.

Note When auto-manage is enabled, after devices are discovered an inventory is run automatically for the auto-managed devices. For more information about auto-manage, see Enable Discovery Options, page 6-18.

Step 5 To view details about a device, select the device from the device selector. The Device Details pane appears. You can change the device's status by using the Manage and Unmanage buttons.

Note Some details may not be displayed if the corresponding parameters are not set on the device; for example, Location and Contact.

The details in the Device Details pane are as follows:

Table 6-1 Device Details Pane

Field	Description
Device Name	Hostname, IP address, or SNMP sysname.
Description	Detailed device description.
Version	Software version installed on the device.
Device Family	Device type.
SysName	The system name.

Downloaded from www.Manualslib.com manuals search engine

Table 6-1 Device Details Pane (continued)

Field	Description
SysObjectId	Unique identifier that identifies the device type.
Location	Where the device is located.
IP Address	Device IP address.
Subnet	Subnet in which the device is located.
Network Segment	The network segment in which the device is located.
Contact	The person to contact for this device.

Step 6 To delete a device, select the device from the device selector or dialog box and click **Delete**.

The device will be removed from the device selector and from all tables (including trend tables).

Related Topics

Managing Device Discovery, page 6-10

Device Name and IP Address Display, page 1-5

View Device Management History

The Historical Operations table shows information on all changes in device state (from unmanaged to managed or vice versa).

Note Your login determines whether you can use this option.

Procedure

Step 1 To view the Historical Operations table, select **Administration** > **Discover** > **Managed Devices** > **Device History**. The following information is displayed:

Downloaded from www.Manualslib.com manuals search engine

Table 6-2 Managed Device History Information

Field	Description
Timestamp	Date and time when the state change occurred.
Device Name	The device's hostname.
IP Address	The device's IP address.
State	The device's state: • New—Device was discovered but has not been moved to the managed or unmanaged state. • Managed—Device has been moved to the managed state. • Unmanaged—Device is unmanaged.

Step 2 To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Specifying Device Credentials

This option allows you specify device community strings and HTTP credentials.

- **SNMP Communities**—Specify community strings for managed devices. See Specify Community Strings, page 6-7.
- **HTTP User/Password**—Specify the HTTP usernames and passwords for configuring access points. See Specify the HTTP Username and Password, page 6-9.

Downloaded from www.Manualslib.com manuals search engine

Specify Community Strings

The Wireless LAN Solution Engine uses a device's read-only community string to discover the device and uses the read/write community string to configure the device. If community strings are not entered correctly, the Wireless LAN Solution Engine cannot communicate with the device. Both read-only and read/write community strings are required.

The default community string is *public* for both the read-only string and the read-write string. If the community strings on your devices differ from the defaults, you must specify the community strings before the discovery process can begin and before you can configure the devices.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > Device Credentials > SNMP Communities**. The SNMP Communities dialog box appears.

This dialog box contains a default entry that covers all devices, provided device community strings are set to the default (*public*).

Step 2 To add new entries, you can enter community strings by using either of the following methods:

- Use the individual text boxes and list for the variables: Hostname (IP address), Read Community, SNMP Timeout, SNMP Retries, and Write Community. Then click **Add**. The community string appears in the large textbox.
- Enter the data directly in the large text box using the following syntax:

  target:*read_community*::*timeout*:*retries*:::*write_community*

  Note You must enter the correct number of colons between variables. Otherwise, the community strings cannot be read.

Information about the variables follows. For more details, see Community String Guidelines, page 6-9.

Downloaded from www.Manualslib.com manuals search engine

Table 6-3 Community String Guidelines

Variable	Description	Notes
target	The IP address of a device or range of devices that use these community strings.	If you do not specify a target, the default community strings apply to all devices in the network.
read_community	A password allowing read-only access to the target devices.	You must specify the read community string. Otherwise, the default value of public is used.
timeout	The length of time (seconds) the server waits for a response from the device before performing the first retry.	The default is 10 seconds. If you increase the timeout period, discovery could take significantly longer to complete. The minimum value is one and the maximum value is 60.
retries	Number of attempts the server makes to communicate with the device before declaring that the device has timed out.	The default is one retry. If you increase the number of retries, discovery takes significantly longer to complete. The default retry policy doubles the previous timeout value for retry.
write_community	The password that allows write access to the target devices.	You must specify the write community string. Otherwise, the default value of public is used.

Step 3 To modify an entry, make your changes directly in the large textbox.

Step 4 Click **Save** to apply your changes.

Related Topic

Community String Guidelines, page 6-9

Downloaded from www.Manualslib.com manuals search engine

Community String Guidelines

Use these guidelines when adding or modifying community strings:

- You can assign community strings to any of the following:
  - Complete IP address; for example, 172.20.4.9
  - Any wild cards (based on IP addresses); for example:

    ..*.*

    172.*.*.*
  - Address ranges, which can include wild cards; for example:

    27.20.[4-55].*

    172.[21-30].[44-88].*

    172.*.*.[121-255]
- You can add a combination of general and specific entries, but the WLSE reads the community strings from most specific to least specific.
- If you enter duplicate community strings for a device, the most specific community string is used.
- A # sign as the first character on a line indicates a comment.
- All printable characters, except for colons (:), are allowed in community strings.
- Spaces are not allowed in community strings.

Specify the HTTP Username and Password

HTTP usernames and passwords are required for downloading configuration files to access points. The password must be set on each access point, and you can enter as many usernames and passwords as necessary on the WLSE. For more information about setting passwords on access points, see Set Up Devices, page 6-12.

Note Your login determines whether you can use this option.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Administration > Discover > Device Credentials > HTTP User/Password**.

Step 2 To add a username and password:

a. Enter the access point IP address or range of IP addresses that will use this username and password.

b. Enter the username.

c. Enter the password.

d. Click **Save**. The IP address and username are added to the Current Entries textbox.

Step 3 To modify an entry:

a. Select the entry from the Current Entries text box.

b. Modify fields as needed and click **Save**.

Step 4 To delete an entry, select it from the Current Entries text box and click **Delete**.

Related Topic

Chapter 3, "Configuring Devices"

Managing Device Discovery

When you select **Administration > Discover > DISCOVER**, the following options appear:

- **Discovery Options**—Enable or disable automatic management of discovered devices and enable or disable reverse DNS lookup (See Enable Discovery Options, page 6-18).
- **Filter Rules**—Limit discovery by setting up IP address filters (See Set Up Discovery Filters, page 6-19).
- **Schedule Discovery**—Set up scheduled discoveries (see Schedule Discovery, page 6-20).

Downloaded from www.Manualslib.com manuals search engine

- **Run Discovery Now**—Run a one-time, immediate discovery (see Run Discovery Now, page 6-22)

You can also view details on the last 15 discoveries—See Viewing Inventory and Discovery Task History, page 6-27.

Related Topics

- Overview: Discovery, page 6-11
- Set Up Devices, page 6-12

Overview: Discovery

You can set up regularly scheduled discoveries and run one-time discoveries.

Before the WLSE can discover devices:

- You must configure discovery on the WLSE. See Schedule Discovery, page 6-20.

  As an alternative to using Cisco Discovery Protocol (CDP) to run discovery, you can import devices from a file or from CiscoWorks2000. See Importing Devices, page 6-28.
- Devices must be properly configured for access by the WLSE. See Set Up Devices, page 6-12.
- Community strings must be entered on the WLSE. See Specify Community Strings, page 6-7).

Note Routers and switches are only discovered if they have properly configured access points attached to them.

Discovery proceeds according to the seed devices and CDP distance that you specify. The CDP distance determines the depth of the discovery. With a CDP distance of 1, only the immediate neighbors of the seed device are discovered. With a CDP distance of 2, devices A and B that are directly connected to the seed device are discovered, and the immediate neighbors of A and B are also discovered. You should set the CDP distance so that your entire wireless network is discovered.

After devices are discovered, you must move them to the managed state. Unmanaged devices do not appear in WLSE displays.

Downloaded from www.Manualslib.com manuals search engine

Related Topic

Importing Devices, page 6-28

Managing Devices, page 6-2

Set Up Devices

You must set up devices so the WLSE can discover and manage them. This section describes both required and optional setup tasks for:

- Set Up Access Points and Bridges, page 6-12
- Set Up Routers and Switches, page 6-15
- Set Up AAA Servers, page 6-16

Set Up Access Points and Bridges

You can set up access points and bridges in two ways:

- By using the WLSE's automatic configuration option for first-time device configuration (select **Configuration > Auto Update**). For more information, see Automating Configurations, page 3-151.
- By opening a web browser session on each device and perform the tasks in the following table. To use this method, you must first configure each access point or bridge for web browsing.

Table 6-4 Set Up Procedures for Access Points and Bridges

Tasks	Procedure	Notes
1. Enable Cisco Discovery Protocol (CDP).	1. In the Summary Status page, click **Setup**. The Cisco Services Setup page appears. 2. Under Services: Cisco Services, click **Cisco Discovery Protocol**. The CDP Setup page appears. 3. Select Enabled. Click **Apply** or **OK**.	CDP is required for the WLSE to discover devices on the network.

Downloaded from www.Manualslib.com manuals search engine

Table 6-4 Set Up Procedures for Access Points and Bridges (continued)

Tasks	Procedure	Notes
2. Enable SNMP. (Optional) Set the location. (Optional) Set the system name and system contact.	1. In the Summary Status page, click **Setup**. The Cisco Services Setup page appears. 2. Under Services, click **SNMP**. The SNMP Setup page appears. 3. Select Enabled. 4. Enter a System Name, System Location, and System Contact. 5. Click **Apply** or **OK**.	SNMP is required for the WLSE to discover and manage the device. Setting the location enables proper grouping of devices into the system-defined Location group. For more information, see Managing Groups, page 6-37. Setting the system name and system location displays this information when you display device details.
3. Set the community string by creating a user with all privileges. (If you already entered an SNMP Admin Community name, the user created has Write, SNMP, Firmware, and Admin privileges, and the User Manager is enabled, you do not need to create another user.)	1. In the Summary Status page, click **Setup**. The Cisco Services Setup page appears. 2. Under Services, click **Security**. The Security Setup page appears. 3. Click **User Information**; then click **Add New User**. The User Management window appears. 4. To create an user with SNMP read/write privileges, enter a username and password and select the Write, SNMP, Firmware, and Admin capabilities. 5. Click **Apply** or **OK**.	The username of the user with write and SNMP privileges is used as the SNMP read/write community string. The Firmware privilege is required for configuring devices from the WLSE.

Downloaded from www.Manualslib.com manuals search engine

Table 6-4 Set Up Procedures for Access Points and Bridges (continued)

Tasks	Procedure	Notes
4. Add an HTTP user with the ability to modify firmware, and enable the User Manager. You can use the same user that you created in Task 3, if the user has firmware privileges.	1. In the Summary Status page, click **Setup**. The Cisco Services Setup page appears. 2. Click **Security**. The Security Setup page appears. 3. Click **User Information**; then click **Add New User**. The User Management window appears. 4. Enter a username and password and select Firmware; then click **Apply**. 5. Navigate back to the Security Setup page and click **User Manager**. The User Manager Setup window appears. 6. Select Enabled; then click **Apply** or **OK**.	This allows configuration uploads from the WLSE to the access point. You must also enter HTTP users and passwords on the WLSE (see Specify the HTTP Username and Password, page 6-9).
5. Set up TFTP as the transfer protocol between the WLSE and access points.	1. In the Summary Status page, click **Setup**. The Cisco Services Setup page appears. 2. Under Services, click **FTP**. The FTP Setup page appears. 3. Use the pulldown menu to select TFTP as the file transfer protocol. 4. In the Default File Server text box, enter the IP address of the WLSE. 5. Click **Apply** or **OK**.	TFTP is used for transferring configuration changes to access points.

Downloaded from www.Manualslib.com manuals search engine

Set Up Routers and Switches

Note Only routers and switches that have properly configured access points or bridges attached to them will be discovered.

On each router and switch, configure the following:

Table 6-5 Set Up Procedures for Routers and Switches

Task	Procedure	Notes
1. Enable CDP and verify that access points and bridges are visible from the router or switch.	1. Enter enable mode. 2. Verify that CDP is running on the switch or router: On IOS-based devices, use the **show cdp run** command. On Hybrid OS-based Catalyst switches, use the **show cdp** command 3. If CDP is not running, use the **set cdp enable** command to enable CDP. 4. To verify that access points or bridges are visible in the device's CDP table, use the **show cdp neighbors** command.	CDP is required for the WLSE to discover the device.
2. Enable SNMP and set up community strings.	On IOS-based devices, enter configuration mode and use the **snmp community** *community_string* **ro** command. On Hybrid OS-based Catalyst devices, enter enable mode and use the **set snmp community read-only** *community_string* command.	SNMP is required for the WLSE to discover and manage the device.

Downloaded from www.Manualslib.com manuals search engine

Table 6-5 Set Up Procedures for Routers and Switches (continued)

Task	Procedure	Notes
3. (Optional) Set the system name, contact, and location variables.	On IOS-based devices, enter configuration mode and use the following commands. • To set the system name, use the **hostname** *name* command. • To set the system contact, use the **snmp contact** *contact* command. • To set the location, use the **snmp location** *location* command. On Hybrid OS-based Catalyst switches, enter enable mode and use the following commands: • To set the system name, use the **set system name** *name* command. • To set the system contact, use the **set system contact** *contact* command. • To set the location, use the **set system location** *location* command.	These variables make the device more manageable. The location variable enables proper grouping of devices into the system-defined Location group. For more information about groups, see Managing Groups, page 6-37. The system name, system contact, and location will appear in the device detail displays.

Set Up AAA Servers

The WLSE can monitor the performance of AAA (Authentication, Authorization, and Accounting) services provided by CiscoSecure ACS Server. To enable monitoring, you must:

- Configure CiscoSecure ACS server to recognize the WLSE as a client. Follow the procedure in this section on each server.
- Configure the WLSE to add information about the LEAP, RADIUS, and EAP-MD5 servers. For more information, see Adding, Modifying and Deleting AAA Servers, page 6-33.

Procedure

Step 1 Log into CiscoSecure ACS Server on a PC that will provide authentication services to the wireless network.

Downloaded from www.Manualslib.com manuals search engine

Note You will need the IP address or name of the PC when configuring the WLSE.

Step 2 Click **User Setup** on the left side of the initial page. The User Setup page appears.

Step 3 Enter a username for the user the WLSE will use for synthetic transactions and click **Add/Edit**.

Step 4 Enter a password in the first set of Password and Confirm Password textboxes. Click **Submit**.

Note You will need this name and password when configuring the WLSE.

Step 5 Click **Network Configuration** on the left side of the page. The Network Configuration screen appears.

Step 6 Click **Add Entry**. In the Add AAA Client area, enter the WLSE information in the following text boxes:

- Client Hostname—enter the WLSE hostname (or IP address)
- Client IP—enter the WLSE IP address
- Key—enter a secret key

Note You will need this key when configuring the WLSE.

Step 7 Select RADIUS (Cisco Aironet) from the Authenticate Using list.

Step 8 Click **Submit** or **Submit+Restart**. A restart is required for the changes to take effect.

Downloaded from www.Manualslib.com manuals search engine

Enable Discovery Options

You can modify the discovery process by specifying that all discovered devices be automatically managed and enabling reverse DNS lookup so that device names, instead of IP addresses, appear in WLSE displays.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > DISCOVER > Discovery Options**. The Discovery Options window appears.

Step 2 To enable automatic management for all discovered devices, select the **Auto-Manage Devices** checkbox.

All discovered devices will be automatically placed in the Managed folder.

Note If you are using the automatic configuration feature (**Configuration > Auto Update**), new access points and bridges added to the network will be automatically configured if Auto-Manage is enabled. For more information, see Automating Configurations, page 3-151.

Step 3 If DNS is configured on devices, you can enable reverse DNS lookup by selecting the Use reverse DNS lookup checkbox. Use of this feature affects device name display on the WLSE as follows:

Reverse DNS lookup enabled?	Affect on Display
Yes	If the lookup succeeds, the device name is displayed.
	If the lookup fails, the device IP address is displayed.
No	If the device's SNMP sysName is set, the sysName is displayed.
	If the sysName is not set, the device IP address is displayed.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Click **Save**.

Related Topics

Manage Devices, page 6-3

Set Up Discovery Filters

You can limit discovery to certain devices by setting up filter rules to include or exclude devices. Filter rules consist of device IP addresses with optional wildcards and ranges.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration** > **Discover** > **DISCOVER** > **Filter Rules**. The Filter Rules window opens.

Step 2 Add IP addresses to the Include Rules or Exclude Rules text boxes, one entry per line. Use standard IP address format (four octets separated by periods) in which any octet can be:

- A value between 0 and 255.
- An asterisk (*) wildcard, denoting any number from 0 to 255; for example, 10.20.*.*.
- A range in which the first number is less than the second; for example, 10.20.30[50-60].

Rules cause discovery to be limited as described in the following table.

Note Exclude rules take precedence over include rules.

Downloaded from www.Manualslib.com manuals search engine

Table 6-6 Effects of Include and Exclude Rules in Discovery Filters

Include Rules Defined?	Exclude Rules Defined?	Result
No	No	All devices are discovered.
No	Yes	All devices are discovered, but those that match the Exclude Rules are discarded.
Yes	No	Only devices that match the Include Rules are discovered.
Yes	Yes	Only devices that match the include rules are discovered. Devices that match the exclude rules are discarded.

For example, assume the IP addresses of the devices in a network are from 10.10.10.1 through 10.10.10.200:

- The include rule is 10.10.10.[40-80]
- The exclude rule is 10.10.10.[60-70]

All of the devices with the IP addresses 10.10.10.[40-80] are discovered, but those with IP addresses 10.10.10.[60-70] are discarded. Therefore, the devices discovered and retained have IP addresses 10.10.10.[40-59] and 10.10.10.[71-80].

Step 3 Click **Save** to save your Rules.

The Rules will take effect for all subsequent discoveries.

Schedule Discovery

This option allows you to schedule discovery. You can specify that scheduled discoveries be repeated at specified intervals. Before discovery can proceed, you must specify at least one seed device. Any supported device can function as a seed. Neighbors of seed devices are discovered by examining the contents of CDP tables.

You may want to specify multiple seed devices to:

- Shorten the discovery time.

Downloaded from www.Manualslib.com manuals search engine

- Discover “disconnected” networks; that is, discover devices across links on which CDP is disabled or discover devices outside the firewall.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > DISCOVER > Schedule Discovery**. The Discovery - Configuring Seeds dialog box appears.

Step 2 To add seed devices, enter their comma-separated IP addresses or device names in the Seed Values text box and click >>. Seed devices that you add in this dialog box will be retained so that you can use them for subsequent scheduled and immediate discoveries.

Device names must resolve to your local DNS in order to translate device names to IP addresses during discovery. The requirements for entering device names are:

- Blank spaces are not allowed.
- The first character in a name must be alphanumeric
- The only valid characters are the alphanumeric characters, the minus sign (-), and the period (.).
- The last character cannot be a minus or a period.

Tip You can add multiple seed devices at one time by copying and pasting seed device names or IP address from a file.

Note Before you can proceed to the next screen, Modify Discovery Schedule, you must have at least one seed device in the Seed Values list.

Step 3 To delete a seed device, select the IP address from the Seed Values list and click **Delete**.

Step 4 Select the CDP distance from the list. Set CDP distance appropriately to discover the entire wireless network; a CDP distance of 1 only discovers the immediate neighbors of the seed devices.

Downloaded from www.Manualslib.com manuals search engine

Note Routers and switches that do not have access points attached to them are used when computing CDP distance. However, such devices will not appear in the discovered devices list.

Step 5 If you have not entered community strings that allow the WLSE to access all devices to be discovered, click **Enter community strings before running discovery**. The SNMP Community dialog box appears. For more information about entering community strings, see Specifying Device Credentials, page 6-6.

Step 6 To schedule discovery, click **Modify Schedule**. The Modify Discovery Schedule dialog box appears.

- Select the State Date and Start Time from the pulldown lists.
- To repeat discovery at specified intervals, click **Enable**. Then enter a number in the Every textbox and select the interval from the list.

Step 7 Click **Next**. The CDP Discovery - Summary dialog box appears.

Step 8 Click **Finish** to submit your settings or **Back** to make changes in your settings.

Related Topic

Specifying Device Credentials, page 6-6

Run Discovery Now

This option allows you to run an immediate, one-time discovery.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > DISCOVER > Run Discovery Now**. The Run Discovery Now - Seeds dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 If necessary, add seed devices:

Note Any seed devices added here are used for this one-time discovery only.

a. Enter the seed device's IP address or device name in the Add Seed Value text box and click >>.

   Device names must resolve to your local DNS in order to translate device names to IP addresses during discovery. The requirements for entering device names are:

   – Blank spaces are not allowed.

   – The first character in a name must be alphanumeric.

   – The only valid characters are the alphanumeric characters, the minus sign (-), and the period (.).

   – The last character cannot be a minus or a period.

b. Set the CDP by selecting a number from the list.

Step 3 If you have not added community strings that allow the WLSE to access all devices to be discovered, click **Enter community strings before running discovery**. The SNMP Community dialog appears. For more information about entering community strings, see Specify Community Strings, page 6-7.

Step 4 Click **Run Now**. The Discovery - Summary dialog box appears.

- Click **Back** if you want to make changes before running the discovery.
- Click **Finish** to run the discovery. The discovery will begin within 2 minutes.

Step 5 The Tasks History window appears. You can expand the Discovery folder to see the results of the discovery:

- Immediate discoveries are named CDPDiscovery_Run_Now_*number*. The *number* increments each time you run an immediate discovery.
- Click the discovery name. The Run Log appears, showing the start and end times of the discovery and information about the devices that were discovered.

Related Topics

- Specifying Device Credentials, page 6-6

Downloaded from www.Manualslib.com manuals search engine

- Viewing Inventory and Discovery Task History, page 6-27

Running Inventories

The WLSE automatically runs scheduled inventories (see About Scheduled Inventories, page 6-24), and you can run immediate inventories of all devices or of selected devices.

When you select **Administration > Discover > Inventory**, the following options for running immediate inventories appear:

- **Run Inventory Now**—Use this option to collect complete inventory data from selected devices (see Immediate Inventory of Selected Devices, page 6-25).
- **Inventory All Devices**—Use this option to collect inventory data from all devices—see Immediate Inventory of All Devices, page 6-26).

You can view details on the last 15 inventories—See Viewing Inventory and Discovery Task History, page 6-27.

About Scheduled Inventories

The WLSE runs 3 types of inventories on a regularly scheduled basis:

- Basic inventories that collect all the information required by the WLSE to populate displays, such as reports, and to place devices in system-defined groups. This inventory runs hourly by default.

  In the inventory history listing, these inventories appear under the name *Inventory*.

- Client inventories that only collect information about associations of clients to access points. This inventory runs every 5 minutes by default.

  In the inventory history listing, these inventories appear under the name *ClientInventory*.

- Performance inventories that only collect the performance attributes used in trend reports for access points, bridges, and AAA servers. This inventory runs every 15 minutes.

  In the inventory history listing, these inventories appear under the name *PerformanceInventory*.

Downloaded from www.Manualslib.com manuals search engine

To change the scheduled inventory intervals, you can reset the inventory polling parameters. See Managing System Parameters, page 6-73.

Immediate Inventory of Selected Devices

Use this option to run an immediate inventory of selected devices.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > Inventory > Run Inventory Now**. The device selector shows all managed devices in group folders in the middle pane, and the Run Inventory Collection window appears.

Step 2 To search for devices:

a. From the list in the search area located in the middle pane, select the method for searching: by device name or IP address.

b. Enter the IP address or name. You can use asterisks (*) as wildcards. An asterisk denotes any number of characters in a name or an entire octet in an IP address; for example, *AP or 172.*.*.*.

c. Click **Search**. The matching devices appear in the Search Results folder in the device selector.

Step 3 To select devices for inventory:

a. Expand the folder that contains the devices you want to include.

b. Click the device group folder. All of the devices in the group are added to the list in the Run Inventory Collection window.

Note Each immediate inventory job for selected devices contains devices from only one group.

c. From the list of devices in the group, select the devices you want to inventory.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Click **Run Inventory for Selected Devices**. The inventory job starts immediately. Managed devices are polled and information is collected. WLSE displays are updated accordingly.

Step 5 The Tasks History window appears. You can expand the Inventory folder to see the results of the inventory collection:

- Inventories of selected devices are named InventoryRunNow_*number*. The *number* increments each time you run an inventory.
- Click the inventory name. The Run Log appears, showing the start and end times of the inventory and the type of data that was collected for the devices you selected.

Immediate Inventory of All Devices

Use this option to run an immediate inventory of all devices. This inventory is the same as the scheduled basic inventory. Inventories that collect data for all devices are named *Inventory*, whether they are scheduled inventories or immediate inventories run by a user.

Note Your login determines whether you can use this option

Procedure

Step 1 Select **Administration** > **Discover** > **Inventory** > **Inventory All Devices**.

Step 2 Click **Inventory All Devices**. The inventory job starts immediately. Managed devices are polled and information is collected. WLSE displays are updated accordingly.

If an inventory is currently running, a message appears. You should wait for the running inventory to complete before starting the immediate inventory.

Step 3 The Tasks History window appears. You can expand the Inventory folder to see the results of the inventory collection.

- Inventories of all devices are named *Inventory*.

Downloaded from www.Manualslib.com manuals search engine

- Click the inventory name. The Run Log appears, showing the start and end times of the inventory and type of data that was collected.

Viewing Inventory and Discovery Task History

You can view the history of inventories and discoveries by using the Task History option. Details on the last 15 inventories and discoveries are accessible through this option.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > Tasks History**. The Tasks selector appears.

Step 2 To view a list of jobs, expand the Discoveries or Inventories folder. A list of the last 15 jobs appears with the latest job listed first and earliest listed last.

The names of the inventory and discovery jobs indicate the type of inventory or discovery as follows:

Table 6-7 Discovery Job Names

Name	Type of Job
CDPDiscovery	Scheduled discoveries.
CDPDiscovery_Run_Now_*number*	Immediate, one-time discoveries.
CDPDiscovery_Import_Devices	Devices were imported from a file or from a CiscoWorks2000 server.

Downloaded from www.Manualslib.com manuals search engine

Table 6-8 Inventory Job Names

Name	Type of Job
Inventory	Scheduled and immediate inventories of all devices.
ClientInventory	Scheduled inventories of client associations to access points.
PerformanceInventory	Scheduled inventories of performance attributes used in trend reports.
InventoryRunNow_*number*	Immediate inventories of selected devices, run by users.

Step 3 To view details about a job, select the job. The Run Log appears, showing the start and end times of the job and type of data that was collected.

Related Topics

- Running Inventories, page 6-24
- Immediate Inventory of Selected Devices, page 6-25
- Immediate Inventory of All Devices, page 6-26

Importing Devices

Instead of running discovery on the WLSE, you can import devices:

- From a file (see Import Devices from a File, page 6-29).
- From CiscoWorks2000 Resource Manager Essentials (see Import Devices from CiscoWorks2000, page 6-30).

A one-time discovery job starts immediately after you import devices. All WLSE-supported devices in the file are used as seed devices with a CDP of 1. These devices are not added to the list of available seed devices in the Discovery - Configuring Seeds dialog box, but they do appear in the Discovery Run Log. See Schedule Discovery, page 6-20 and Viewing Inventory and Discovery Task History, page 6-27.

Downloaded from www.Manualslib.com manuals search engine

Devices not supported by the WLSE are ignored.

You can choose to discover some devices and import others.

The following information is imported:

- IP addresses are accepted, and hostnames are resolved to obtain the IP address. Hostnames that cannot be resolved are ignored.
- Read-only and read/write community strings are appended to the end of the Bulk SNMP Settings table (**Administration > Discover > Device Credentials**). See Specifying Device Credentials, page 6-6.

Note Imported credentials are not matched with existing entries that contain wildcards or ranges.

Import Devices from a File

You can import devices from a file that contains device information in the CSV format. You can create a CSV file by exporting devices from CiscoWorks2000 or by creating the file with a text editor. You can view a sample CSV file in the dialog box for importing files.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > Import Devices > From File**. The Import Devices from File dialog box appears.

To see a sample file, click **See Sample CSV File**.

Step 2 You can enter a pathname for the file in the Choose File dialog box or click Browse to find the file in the client directory structure.

Step 3 Click **Import**. Devices are imported and a one-time discovery begins within 2 minutes.

Downloaded from www.Manualslib.com manuals search engine

Step 4 To verify the discovery, see Viewing Inventory and Discovery Task History, page 6-27.

Related Topics

- Import Devices from CiscoWorks2000, page 6-30
- Schedule Discovery, page 6-20
- Specifying Device Credentials, page 6-6
- Viewing Inventory and Discovery Task History, page 6-27

Import Devices from CiscoWorks2000

You can import devices directly from CiscoWorks2000 by connecting to a CiscoWorks2000 server.

The time required to import devices depends on the response from the CiscoWorks2000 server and the number of devices imported. The following procedure explains how to check the status of the operation.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > Import Devices > From CiscoWorks2000**.

Step 2 Enter the following information. All fields are required; if any are left blank, the display will clear.

- The CiscoWorks2000 server IP address.
- The port number at which the CiscoWorks2000 server listens for HTTP requests. You may need to contact the administrator of the CiscoWorks2000 server to obtain this information.
- The username and password of any user who has the authority to export and import device credentials on the CiscoWorks2000 server.

Click **Import**. After devices are imported, a one-time discovery begins.

Downloaded from www.Manualslib.com manuals search engine

Step 3 To see the Import Status log, click **Status**. The CiscoWorks2000 Import Status window appears. To refresh the status display, click **Refresh**.

- If the Last Status button is displayed in place of the Status button, you can review the results of a previous import.
- If the import fails because you entered the wrong data in the Import dialog box, one of the following error messages is included in the Import Status log:
  - The following message means that either the host or the port specified in the WLSE import dialog was wrong:

    Error: Could not connect to CiscoWorks2000 server:*ip_address* on port:*port_number*.
  - The following message means that either the user or password specified in the WLSE import dialog was wrong:

    Error: Connected to CiscoWorks2000 server:*ip_address* on port:*port_number* successfully, but server returned error after connection.
- If the import succeeds, you can view detailed information in the Discovery Run Log. See Viewing Inventory and Discovery Task History, page 6-27.

Related Topics

- Import Devices from a File, page 6-29
- Schedule Discovery, page 6-20

Exporting Devices

You can export all WLSE-discovered devices to a CiscoWorks2000 server running Resource Manager Essentials. The information exported consists of the device IP addresses and their credentials.

The time required to export devices depends on the number of devices exported and the response from the CiscoWorks2000 server. The following procedure explains how to check the status of the operation.

Note Your login determines whether you can use this option.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Administration > Discover > Export Devices > To CiscoWorks2000**.

Step 2 Enter the following information:

- The CiscoWorks2000 server IP address.
- The CiscoWorks2000 server port number. You may need to contact the administrator of the CiscoWorks2000 server.
- The username and password of any user who has the authority to export and import device credentials on the CiscoWorks2000 server.

Step 3 Click **Export**.

The Export to CiscoWorks2000 Started window appears.

Step 4 To see the export status log, click **Status**. The CiscoWorks2000 Export Status window appears. To refresh the status display, click **Refresh**.

If the Last Status button is displayed in place of the Status button, you can review the results of a previous export.

The following information is included in the export status log:

Type of Information	Description
Device information	Name of the device, device status, and device status details. The string !{[NO VALUE]}! does not indicate an error; it means information was not available to the CiscoWorks2000 server while it was sending a response to the WLSE.
Error messages	The following message means that either the host or the port specified in the WLSE export dialog was wrong: Error: Could not connect to CiscoWorks2000 server:*ip_address* on port:*port_number*.
	The following message means that either the user or password specified in the WLSE export dialog was wrong: Error: Connected to CiscoWorks2000 server:*ip_address* on port:*port_number* successfully, but server returned error after connection.

Downloaded from www.Manualslib.com manuals search engine

Step 5 After you export devices, you can view them in CiscoWorks2000 Resource Manager Essentials (see the Resource Manager Essentials online help for details).

Adding, Modifying and Deleting AAA Servers

Before adding AAA servers to the WLSE, you must configure the servers to add the WLSE as a client. For information on adding the WLSE as a client on AAA servers, see Set Up AAA Servers, page 6-16.

After you add AAA servers to the WLSE, the WLSE automatically performs periodic logins on each server to monitor the server's response time and availability.

To add, modify, and delete servers on the WLSE, see the following:

- Manage LEAP Servers, page 6-33
- Manage RADIUS Servers, page 6-35
- Manage EAP-MD5 Servers, page 6-36

For information about changing the polling interval and response time fault thresholds for AAA server monitoring, see Specifying Fault Thresholds, page 2-15.

Related Topics

- Displaying Faults, page 2-1
- Setting Server Response Time, page 2-19
- Specifying Fault Thresholds, page 2-15
- Notification Settings, page 2-20

Manage LEAP Servers

Note Your login determines whether you can use this option.

Procedure

To add, modify or delete a LEAP server:

Downloaded from www.Manualslib.com manuals search engine

Step 1 To add a LEAP server:

a. Select **Administration** > **Discover** > **LEAP SERVER** > **Add Server**. The LEAP Server: Add Server dialog box appears.

b. Complete the following:

Text Box	Description
Server Name	Name or IP address of the AAA server.
Server Port	Port on the server that is used for authentication; this is always 1645.
Username	Client username that you entered on the AAA server.
Password	Client password that you entered on the AAA server.
Secret	Shared secret key that you entered on the AAA server.

c. To add the server, click **Submit**. To clear all data from the textboxes, click **Reset**.

Step 2 To modify a LEAP server:

a. Select **Administration** > **Discover** > **LEAP Server** > **Modify Server**. The LEAP Server: Modify Server dialog box appears.

b. Select a server from the Server Name list, and enter data as described in Step 1.

c. Click **Submit**.

Step 3 To remove a LEAP server:

a. Select **Administration** > **Discover** > **LEAP Server** > **Remove Server**. The LEAP Server: Remove Server dialog box appears.

b. From the list, select the server you want to remove, then click **Submit**.

Step 4 For information on setting the polling interval and response time fault thresholds for LEAP servers, see Specifying Fault Thresholds, page 2-15.

Downloaded from www.Manualslib.com manuals search engine

Manage RADIUS Servers

Note Your login determines whether you can use this option.

Procedure

To add, modify or delete a RADIUS server:

Step 1 To add a RADIUS server:

a. Select **Administration > Discover > RADIUS SERVER > Add Server**. The RADIUS Server: Add Server dialog box appears.

b. Complete the following:

Text Box	Description
Server Name	Name or IP address of the AAA server.
Server Port	Number of the port on the server that is used for authentication; this is always port 1645.
Username	Client username that you entered on the AAA server.
Password	Client password that you entered on the AAA server.
Secret	Shared secret key that you entered on the AAA server.

c. To add the server, click **Submit**. To clear all data from the textboxes, click **Reset**.

Step 2 To modify a RADIUS server:

a. Select **Administration > Discover > RADIUS Server > Modify Server**. The RADIUS Server: Modify Server dialog box appears.

b. Select a server from the Server Name list, and enter data as described in Step 1.

c. Click **Submit**.

Step 3 To remove a RADIUS server:

a. Select **Administration > Discover > RADIUS Server > Remove Server**. The RADIUS Server: Remove Server dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

b. From the list, select the server you want to remove, then click **Submit**.

Step 4 For information on changing the polling interval and response time fault thresholds for RADIUS servers, see Specifying Fault Thresholds, page 2-15.

Manage EAP-MD5 Servers

Note Your login determines whether you can use this option.

Procedure

To add, modify or delete a EAP-MD5 server:

Step 1 To add an EAP-MD5 server:

a. Select **Administration > Discover > EAP-MD5 SERVER > Add Server**. The EAP-MD5 Server: Add Server dialog box appears.

b. Complete the following:

Text Box	Description
Server Name	Name or IP address of the AAA server.
Server Port	Number of the port on the server that is used for authentication; this is always port 1645.
Username	Client username that you entered on the AAA server.
Password	Client password that you entered on the AAA server.
Secret	Shared secret key that you entered on the AAA server.

c. To add the server, click **Submit**. To clear all data from the textboxes, click **Reset**.

Step 2 To modify an EAP-MD5 server:

a. Select **Administration > Discover > EAP-MD5 Server > Modify Server**. The EAP-MD5 Server: Modify Server dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

b. Select a server from the Server Name list, and enter data as described in Step 1.

c. Click **Submit**.

Step 3 To remove an EAP-MD5 server:

a. Select **Administration > Discover > EAP-MD5 Server > Remove Server**. The RADIUS Server: Remove Server dialog box appears.

b. From the list, select the server you want to remove, then click **Submit**.

Step 4 For information on changing the polling interval and response time fault thresholds for EAP-MD5 servers, see Specifying Fault Thresholds, page 2-15.

Managing Groups

When you select **Administration > Group Management**, the device selector appears in the left pane and a group management window appears in the right pane. Initially, only the system-defined groups appear in the device selector. The group management window allows you to create your own groups—see Creating, Editing, and Deleting Groups, page 6-39).

Related Topics

- Overview: Groups, page 6-37
- Creating, Editing, and Deleting Groups, page 6-39

Overview: Groups

The Group Management window allows you to view the existing device groups and categorize devices into named groups so that you can perform management tasks on a group of devices as a single operation.

A group is a named entity that can contain devices, other groups, or a combination of devices and groups. There are two types of groups:

- System-defined groups—See System-Defined Groups, page 6-38.
- User-defined groups—See User-Defined Groups, page 6-39.

Downloaded from www.Manualslib.com manuals search engine

The device selector lists all the current groups, both system-defined groups and user-defined groups. The number after a group name or folder shows how many objects are in the group (devices and other groups) or how many groups are in the folder. Every managed device appears in one or more of the system-defined groups, and may also appear in user-defined groups.

System-Defined Groups

There are six system-defined folders containing system-defined groups.

You cannot edit or delete a system-defined group. The system defined groups are automatically populated using information read from the devices during discovery and inventory collection. Any changes on devices are reflected in the system-defined groups only after the next discovery or inventory collection has completed. The system-defined groups and folders are:

- Device Type folder—Contains groups for AAA servers, 1200 APs, 340 APs, 350 APs, 350 Bridges, Routers, and Switches.

  Note 4800 APs will appear in the system folder for 350 APs.

- Location folder—Contains groups based on the locations of the devices. To enable creation of system-defined location groups, you must configure a parameter on the device that identifies the device location. See Set Up Devices, page 6-12 for information on setting location. The *null* location group contains all devices that are not configured with their location information.
- SSID folder—Contains a group for each primary radio service set ID (SSID) configured on access points. For information on configuring the SSID, see Set Up Devices, page 6-12
- Software Version folder—Contains a group for each software version detected on the devices.
- Subnet folder—Contains a group for each subnet configured in the network.
- VLAN folder—Contains a group for each VLAN configured on the access points.

Downloaded from www.Manualslib.com manuals search engine

User-Defined Groups

You can define any number of groups, which can contain subgroups and devices. User-defined groups can contain devices and other groups, so you can set up hierarchies of groups.

Related Topics

- Creating, Editing, and Deleting Groups, page 6-39
- Managing Device Discovery, page 6-10
- Running Inventories, page 6-24

Creating, Editing, and Deleting Groups

You can create groups and edit or delete user-defined groups. The system-defined groups cannot be edited or deleted.

Use the options in the group management window to:

- Add a Group, page 6-39
- Edit a Group, page 6-42
- Delete a Group, page 6-43

To view the devices in a group, select **Administration > Group Management**. Expand the folders or groups until you can click on the group you want to view. The group name, description, creator, and devices are listed in the Members area of the group management window.

Add a Group

You can add groups by:

- Creating a New Group, page 6-40
- Copying an Existing Group, page 6-41

Note Your login determines whether you can use this option.

Downloaded from www.Manualslib.com manuals search engine

Creating a New Group

Procedure

Step 1 Select **Administration > Group Management**. The group selector pane and group window are displayed.

Step 2 To create a new group, click **Create New**. The Create Group dialog appears and the Search dialog appears above the group selector. To search for devices:

a. From the list in the search dialog, select the method for searching: by device name or IP address.

b. Enter the IP address or name. You can use asterisks (*) as wildcards. An asterisk denotes any number of characters in a name or an entire octet in an IP address; for example, *AP or 172.*.*.*.

c. Click **Search**. The matching devices appear in the Search Results folder in the device selector.

Step 3 Enter a name in the Name text box. Enter a description in the Description text box (optional).

For information about the characters allowed in group names and descriptions, see Naming Guidelines, page A-1.

Step 4 To make your new group a subgroup of another group, select a group from the Subgroup Of list. By default, all new groups are added at the top level ([root]).

Note Your new group will be added to the **Subgroups Of** list.

Step 5 From the group selector in the left pane, select a group that contains devices you want to add to your new group. Devices in that group are added to the Available Devices list in the Create Group dialog.

Step 6 To add devices to the new group, select the group or individual devices from the All Available Devices list and click >>. Devices are moved to the Devices in Group list.

Step 7 To add more devices to the new group, repeat Steps 5 and 6.

Step 8 To remove devices from the group, select them from the **Devices in Group** list and click <<.

Downloaded from www.Manualslib.com manuals search engine

Step 9 To save the group, click **Save**. The new group is displayed and added to the end of the group selector list. To cancel the group creation and discard your changes, click **Cancel**.

Copying an Existing Group

Use this procedure to create a new group by copying an existing group. You can copy both system groups and user-defined groups.

Procedure

Step 1 Select **Administration > Group Management**. The group selector pane and group dialog box are displayed.

Step 2 To copy an existing group, select the group and click **Copy**:

The Copy Group dialog appears. The devices in the group are placed in the Devices in Group list.

The Search dialog appears above the device selector. To search for devices:

a. From the list in the search dialog, select the method for searching: by device name or IP address.

b. Enter the IP address or name. You can use asterisks (*) as wildcards. An asterisk denotes any number of characters in a name or an entire octet in an IP address; for example, *AP or 172.*.*.*.

c. Click **Search**. The matching devices appear in the Search Results folder in the device selector.

Step 3 Edit the name, if desired. Change or add the description in the Description text box (optional).

For information about the characters allowed in group names and descriptions, see Naming Guidelines, page A-1.

Step 4 To make the group a subgroup of another group, select a group from the Subgroup Of list. By default, all new groups are added at the top level ([root]).

Note Your new group will be added to the **Subgroup Of** list.

Downloaded from www.Manualslib.com manuals search engine

Step 5 To add more devices to the group:

a. Select another group. Devices in that group are added to the All Available Devices list in the Create Group dialog.

b. Select the group or individual devices from the **Available Devices** list and click >>.

c. To add more devices, repeat Steps a and b.

Step 6 To remove devices from the group, select them from the Devices in Group list and click <<.

Step 7 To save the group, click **Save**. The new group is displayed and added to the end of the device selector list. To cancel group creation and discard your changes, click **Cancel**.

Related Topics

- Edit a Group, page 6-42
- Delete a Group, page 6-43
- Overview: Groups, page 6-37

Edit a Group

You can edit user-defined groups, but system-defined groups cannot be edited.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Group Management**. The group selector pane and Group dialog box appear.

Select a group to edit from the group selector in the left pane and click **Edit**. The Edit Group dialog appears in the right pane and the search dialog appears in the middle pane. To search for devices:

a. From the list in the search dialog, select the method for searching: by device name or IP address.

Downloaded from www.Manualslib.com manuals search engine

b. Enter the IP address or name. You can use asterisks (*) as wildcards. An asterisk denotes any number of characters in a name or an entire octet in an IP address; for example, *AP or 172.*.*.*.

c. Click **Search**. The matching devices appear in the Search Results folder in the device selector.

Step 2 Change the Name or Description by editing the text in the text boxes.

For information about the characters allowed in group names and descriptions, see Naming Guidelines, page A-1.

Step 3 To make the group a subgroup of another group, select a group from the Subgroup Of list. The group you are editing will become a subgroup of the group you select.

Step 4 To add devices to the group, select a group from the group selector. The devices in the group appear in the All Available Devices list. Select the group or individual devices from the list and click **Add**. Devices are placed in the Devices in Group list.

Step 5 To add more devices, repeat Step 4.

Step 6 To delete devices from the group, select one or more devices from the Devices in the Group list and click **Remove**.

Step 7 To save your changes, click **Save**. The edited group is displayed. To discard your changes, click **Cancel**.

Related Topics

- Add a Group, page 6-39
- Delete a Group, page 6-43
- Overview: Groups, page 6-37

Delete a Group

You can delete user-defined groups, but you cannot delete system-defined groups.

Note Your login determines whether you can use this option.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Administration > Group Management**. The device selector appears in the left pane and the Group window appears.

Step 2 Select the group from the group selector list. The group is displayed.

Step 3 Click **Delete**.

Related Topic

- Overview: Groups, page 6-37
- Edit a Group, page 6-42
- Add a Group, page 6-39

Managing the Appliance

Options under the Appliance subtab allow you to manage the WLSE system and use connectivity tools. When you select **Administration > Appliance**, the following options are displayed:

- **Status**—Gather and view WLSE statistics and restart the machine (see Viewing WLSE Status, page 6-45).
- **Software—**Update, reinstall, view status, and define the repository for the WLSE software (see Managing the Software, page 6-47).
- **Security**—Manage WLSE security features, such as telnet, SSL, and authentication modules (see Managing Security, page 6-56).
- **Backup and Restore**—Configure backup location, backup data, and restore data (see Backing Up and Restoring Data, page 6-61).
- **Diagnostics**—Troubleshoot, run self-tests, view process status (see Using Diagnostics, page 6-64).
- **Splash Screen**—Customize the splash screen message (see Setting Up the Splash Screen Message, page 6-69).

Downloaded from www.Manualslib.com manuals search engine

- **Time/NTP/Name**—Set the current time (see Setting the Current Time and Date on the WLSE, page 6-69), specify NTP servers (see Specifying NTP Time Servers, page 6-70), and specify IP name servers (see Specifying Name Servers, page 6-71).
- **Configure Mailroute**—Specify an SMTP server for handling email notifications (see Specifying an SMTP Mail Server, page 6-71).
- **Connectivity Tools**—Test device connectivity and reachability and troubleshoot nonresponding devices (see Using Connectivity Tools, page 6-72).

Note Your login determines whether you can use these options.

Viewing WLSE Status

The Status options include:

- Viewing log file statistics (see Viewing Log File Reports, page 6-45).
- Restarting the WLSE (see Restarting the Wireless LAN Solution Engine, page 6-47).

Viewing Log File Reports

This option allows you to view the contents of WLSE log files.

Procedure

Step 1 Select **Administration > Appliance > Status > View Log File.** The Log File Utilities dialog box appears with the following information:

Field	Description
Log file	Name of the log file displayed.
Directory	Location of log file.
File Size	Size of file.

Downloaded from www.Manualslib.com manuals search engine

Field	Description
Size Limit	Recommended maximum file size.
File Size Utilization %	Percentage of the maximum size (500MB) that is being used.

Step 2 To see log file details, click the name of the log file. A window appears with log file information. For a description of each file, see Log Files Displayed, page 6-46.

Step 3 To search for specific data within the log files, click the check boxes of the log files you want to search, and enter a keyword into the Keyword text box. Click **Case Sensitive** if you want your search to be case sensitive, then click **Search**. A window displays the results of the search.

Log Files Displayed

The WLSE maintains the following log files.

Log File	Content
access_log	Web server user access log.
daemons.log	Log file for logging messages that dmgtd does not log.
dmgtd.log	Process Management daemon log file.
error_log	Web server error log.
faults.log	Log for device fault information.
install.log	Software package installation log.
jobvm.log	Log for all scheduled tasks.
mfgtest.log	Log for the manufacturing test.
mod_jk.log	Message log for hook between Tomcat and Apache.
snmpd.log	SNMP agent log file.
ssl_request_log	Log for secure socket layer web server events for https.
tomcat.log	Java servlet messages.

Downloaded from www.Manualslib.com manuals search engine

Restarting the Wireless LAN Solution Engine

This option allows you to restart the WLSE.

After the Wireless LAN Solution Engine restarts, discovery and inventory will resume at the next scheduled time.

Procedure

Step 1 Select **Administration** > **Appliance** > **Status** > **Restart**. The Restart System screen appears.

Step 2 Click **OK** to restart the Wireless LAN Solution Engine.

Note If you need to perform a manual soft restart (for example, when modifying a network interface) you can use the CLI commands. (Refer to *User Guide for the CiscoWorks1105 Wireless LAN Solution Engine*—From the Online Help, click **View PDF**.)

Related Topics

- Managing Device Discovery, page 6-10
- Running Inventories, page 6-24

Managing the Software

The Software options are:

- **Status**—Currently installed software information, such as software description, installation date, and installation status (see Viewing Software Status, page 6-48).
- **Define Repository**—Specify the repository location. The repository provides software update services to the WLSE (see Defining the Repository, page 6-49).

Downloaded from www.Manualslib.com manuals search engine

- **Software Updates**—Select and install a software update from the repository. You must specify the repository before updating software so the Wireless LAN Solution Engine can locate the software updates (see Installing Software Updates, page 6-52).
- **Browse Repository**—Browse the available complete images and software upgrades on the repository (see Browsing the Repository, page 6-53).
- **Software Update History**— Information about current and previous versions of installed software, including version number, install date, and installation status (see Viewing Software Update History, page 6-54).

Viewing Software Status

You can view information about the software currently installed on the WLSE.

Procedure

Step 1 Select **Administration** > **Appliance** > **Software** > **Status**. The Software Status window appears with the Installed Software table, which contains the following information about all the software currently installed on the WLSE:

Field	Description
Software Name	Brief description of the software.
Installation Date	Date and time (UTC) the software was installed.
Status	Status of the installation.
Details	Detailed install log for this software.

The Last Installation Information table displays the following about the most recent software installation:

Field	Description
Name	Brief description of the software.
Installation Status	Status of the installation.
Log File	Detailed install log for this software.

Downloaded from www.Manualslib.com manuals search engine

Step 2 To view details about an installation, click **View Log** in the Details field.

The install log for the selected installation opens. The information about the latest software installed is displayed.

Related Topics

- Viewing Software Update History, page 6-54
- Installing Software Updates, page 6-52
- Managing the Software, page 6-47

Defining the Repository

The repository warehouses the available software updates for the WLSE. The repository can be either local (on the WLSE), or remote (on a Windows NT or Windows 2000 server). The default is a local repository.

By defining the repository, you are telling the WLSE where to look for available software updates. You can download software from the repository and install it on the WLSE, and you can browse the available software versions on the repository.

Before you can define the repository, you must first it:

- To create a local repository, see Creating a Local Repository, page 6-50.
- To create a remote repository, see Creating a Remote Repository, page 6-51.

Procedure

Step 1 Select **Administration > Appliance > Software > Define Repository**. The Define Repository dialog box appears.

Step 2 To define or redefine the repository, complete the following:

Text Box	Description
Host Name	The hostname or IP address of the repository. For the local repository, enter **`localhost`**.

Downloaded from www.Manualslib.com manuals search engine

Text Box	Description
Port Number	The port number used by the software on the repository. The default port number for the local repository is 9851.
Description	A description of the repository. This text box is optional; you can enter any description.

Step 3 Click **Connect to Repository** to verify that the hostname and port number you entered are correct. If the data is incorrect, an error message appears.

Related Topics

- Installing Software Updates, page 6-52
- Browsing the Repository, page 6-53
- Managing the Software, page 6-47

Creating a Local Repository

A WLSE can serve as the repository for itself and multiple other WLSEs.

To create a local repository, configure the repository using the CLI.

Note To use the local repository, you must be downloading software updates from an FTP site.

For more information, see the *Hardware Installation and Configuration Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*.

Procedure

Step 1 Open a CLI window to the Wireless LAN Solution Engine, using Telnet or SSH.

Step 2 Specify the FTP site that will be the source of the software updates. Use the following CLI command:

repository source ftp://*hostname/path*

Step 3 Find the software you want on the FTP site.

Downloaded from www.Manualslib.com manuals search engine

Step 4 Download the software you want to the repository using the following command:

repository add *package*

Creating a Remote Repository

A remote repository can serve as the repository for one or more Wireless LAN Solution Engines. The remote repository can be either:

- A WLSE functioning as the remote repository for other WLSEs.
- A Windows NT or Windows 2000 server. A remote repository created on a Windows NT or Windows 2000 server will be temporary; it will not exist after the server reboots.

Note If you are using a Wireless LAN Solution Engine as a remote repository, see Creating a Local Repository, page 6-50.

Procedure

Step 1 Download the ZIP file containing the update. The latest updates can be found at ftp.cisco.com.

Step 2 Extract the file to any empty directory. For example, extract the file to C:\wlse\wlse_repository.

Step 3 Open a command window and enter the following command:

```
subst <drive2:><drive1:>\<path>
```

Note Drive2 is a virtual drive. It will be removed after you reboot the Windows 2000 or Windows NT server.

Step 4 Open <drive2:>.

Step 5 If Autoplay is enabled, the autorun.bat file will automatically run. If it does not, double-click it. A browser window opens, displaying the Appliance Update screen.

Downloaded from www.Manualslib.com manuals search engine

Step 6 Enter the hostname or IP address of the appliance.

The remote repository is now on the Windows NT or Windows 2000 server. To install software updates from this repository, see Installing Software Updates, page 6-52.

Related Topic

Creating a Local Repository, page 6-50

Installing Software Updates

Note When you update or reinstall software, the WLSE stops and restarts. Therefore, you cannot access the WLSE during a software update, and you must log in again after updating software.

Procedure

Step 1 Select **Administration > Appliance > Software > Install Software Updates**. The Install Software Updates window opens and displays information about the Wireless LAN Solution Engine, the currently defined repository, and the compatible software available for updating.

Step 2 Select a software version from the Compatible Updates table, Compatible Reinstallations table, or Complete Images table.

These tables display the following information about the software you can install.

Field	Description
Name	Software identifier.
Version	Version number of the software.
Summary	Brief description of the software.
Release Date	Release date of the software.
Details	Detailed description of the software.

Downloaded from www.Manualslib.com manuals search engine

Step 3 To view details about any of the listed software, click **README** in the Details field.

Step 4 To begin the installation, make a selection from the Compatible Updates table, Compatible Reinstallations table, or Complete Images table.

Step 5 To install the selected software, click **Install**. The Install Software Updates window opens.

Step 6 Click **Confirm** to continue the installation. Click **Cancel** to cancel the installation.

When the installation is complete, the WLSE will be unavailable for a few minutes while it restarts. The Login screen will appear when the update is complete.

You can view details of the installation after the installation is complete (**Administration > Appliance > Software > Status >View Log**).

Related Topics

- Defining the Repository, page 6-49
- Viewing Software Status, page 6-48
- Viewing Software Update History, page 6-54
- Browsing the Repository, page 6-53
- Managing the Software, page 6-47

Browsing the Repository

You can browse the available complete images and software upgrades on the repository using this option.

Note A repository must be defined in order to browse software. To define the repository, see Defining the Repository, page 6-49.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Administration > Appliance > Software > Browse Repository**. The Browse Repository dialog box appears.

Step 2 To view detailed information about a complete image or update, click **README** in the Complete Images table or Updates table. These tables display the following about all the software available on the repository:

Field	Description
Name	Software identifier.
Version	Version number of the software.
Appliance Type	The appliance type that the software is designed for.
Release Date	Release date of the software.
Summary	Brief description of the software.
Details	Detailed description of the software. Click **README** to display details.

Related Topics

- Installing Software Updates, page 6-52
- Managing the Software, page 6-47

Viewing Software Update History

This window shows only the update history, not a history of installed images. If you install a complete new image, the previous update history will be erased.

Procedure

Step 1 Select **Administration > Appliance > Software > Software Update History**. The Software Update History window displays the following:

Downloaded from www.Manualslib.com manuals search engine

Table 6-9 Software Update History Window

Field	Description
Name	Software identifier.
Version	Software version.
Summary	Summary of the installed software.
Install Date	The date and time (UTC) the software was installed.
Status	The status of the installed software.
Details	The detailed install log for this software.
Status	The status of the installation: Success—Software was installed with no errors. Warning—Software installed successfully with minor errors. Error—Software installation was unsuccessful.
Details	The detailed install log for this installation, including warning and error messages.

Step 2 Click **View Log** in the Details field to view the detailed install log for a software installation.

Related Topics

- Viewing Software Status, page 6-48
- Browsing the Repository, page 6-53
- Managing the Software, page 6-47

Overview: Security

The WLSE provides the following security features:

- Optional secure connection through a Web browser
- Connection through the CLI via Telnet
- Secure connection through the CLI via SSH

Downloaded from www.Manualslib.com manuals search engine

- Authentication through the local database or through alternative authentication services
- Flexible user access to managed devices and Wireless LAN Solution Engine services through configurable roles.

You can manage your system's security by:

- Selecting an Authentication Module, page 6-57
- Disabling or Enabling Telnet and Selecting SSH, page 6-59
- Viewing the Last 10 Logged-On Users, page 6-60
- Administering Users, page 6-75

Managing Security

The Security options include:

- **Authentication Modules**—Choose the authentication module used (see Overview: Authentication Modules, page 6-56).
- **SSL (HTTPS)**—Obtain a permanent, signed Certificate Signed Request for secure Web access (see Managing SSL (HTTPS), page 6-58).
- **Telnet and SSH**—Configure Telnet and SSH settings (see Disabling or Enabling Telnet and Selecting SSH, page 6-59).
- **Last 10 Logins**—View information about the last 10 users who have logged on to the WLSE (see Viewing the Last 10 Logged-On Users, page 6-60).

Overview: Authentication Modules

The Wireless LAN Solution Engine provides a mechanism for authenticating users through the local authentication module and a local database of user IDs and passwords. Many network managers, however, already have an authentication service. To use your own authentication service instead of the local module, you can select one of the alternative modules:

- TACACS+
- Radius
- MS NT Domain

Downloaded from www.Manualslib.com manuals search engine

After you select and configure a module, all authentication transactions are performed by the authentication service associated with that module. Users log in with the user ID and password associated with the current authentication module.

The Wireless LAN Solution Engine determines user roles; therefore, all users must be in the local database of user IDs and passwords. A user's role determines the services and devices that the user can access. Users must have the same user ID locally as they have in the alternative authentication source, but the local password and authentication service password do not have to be same.

Users who are authenticated by an alternative service and who are not in the local database have no roles assigned to them. Users who have no roles see only the splash screen after logging in and cannot view screens or perform tasks.

If the alternative authentication service fails, the Wireless LAN Solution Engine defaults to the Local authentication module. Even if the local user database fails, you can always log in as the admin user.

Related Topics

- Selecting an Authentication Module, page 6-57
- Administering Users, page 6-75

Selecting an Authentication Module

The Local login module is selected by default, but you can select a different module.

Procedure

Step 1 Select **Administration > Appliance > Security > Authentication Modules**. The Authentication Modules dialog box appears.

Step 2 Select an authentication module from the Select Module drop down list, then click **Submit**. A Configuration dialog box appears for all selections except the Local module.

Step 3 Depending on the authentication module you selected, enter the following data, then click **Submit**:.

- Radius module or TACACS+ module:

Downloaded from www.Manualslib.com manuals search engine

  - Primary Server and Secondary Server—IP addresses or device names of the primary and secondary authentication servers. A secondary server is optional.
  - Shared Secret—Secret key.
- MS NT Domain module:
  - Domain—Name of the Windows domain.
  - Primary Domain Controller and Backup Domain Controller—Names of the primary and backup Windows domain controllers. A backup domain controller is optional.

After you change the authentication module, you do not have to restart the Wireless LAN Solution Engine. Changing the module does not affect users who are currently logged on. Users who log on after the change use the new module.

Related Topic

Overview: Security, page 6-55

Managing SSL (HTTPS)

SSL (secure socket layer) protocol provides a secure connection between Web clients and the Wireless LAN Solution Engine. When you initially set up the Wireless LAN Solution Engine, an unsigned certificate and a CSR (Certificate Signed Request) are automatically generated and SSL is enabled. The unsigned certificate expires in one year. To obtain a permanent, signed certificate, use the following procedure.

Note To establish a connection to the Wireless LAN Solution Engine using SSL, use the prefix https instead of http when entering the URL into the browser and do not append a port number to the URL.

Procedure

Step 1 Select **Administration** > **Appliance** > **Security** > **SSL (HTTPS)**. The SSL (HTTPS) dialog box appears.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Click **View CSR**. The encrypted CSR is displayed.

Step 3 Copy the encrypted CSR (between the *begin* and *end* lines). Send the CSR to a certificate authority (such as Verisign), following the authority's procedure.

Step 4 When you receive the signed certificate:

a. Copy it into an ASCII file on a client system.

b. On the same client, select **Administration > Security**.

c. Under SSL (HTTPS), type the path to the signed certificate or click **Browse** to locate the file, then click **Submit Certificate**.

d. To use the new certificate, you need to restart the Wireless LAN Solution Engine by logging on through the CLI, running the **services stop** command to stop the system, then running the **services start** command to restart the system.

Step 5 You should block login through the regular HTTP port (1741):

a. Log in to the WLSE through the console or by using Telnet or SSH.

b. Enter the following CLI command:

```
# firewall eth0 1741
```

For more information on this command, see the *User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*; from the online help, click **View PDF**.

Related Topic

Overview: Security, page 6-55

Disabling or Enabling Telnet and Selecting SSH

Telnet is used for connecting to the Wireless LAN Solution Engine through the CLI. By default, Telnet is enabled. To prevent unsecure connections through the CLI, you can disable Telnet.

SSH provides a secure Telnet connection, encrypting all traffic, including passwords. By default, both SSH1 and SSH2 are used.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Administration > Appliance > Security > SSH and Telnet**. The SSH and Telnet control panel appears.

Step 2 To change the type of SSH used, select the desired SSH version from Select Protocol, then click **Change Protocol**.

Step 3 To enable or disable Telnet, make a selection from Telnet, then click **Configure**.

Changes takes place immediately.

Related Topic

Overview: Security, page 6-55

Viewing the Last 10 Logged-On Users

You can view information about the last 10 users who have logged on to the WLSE.

Procedure

Step 1 Select **Administration > Appliance > Security > Last 10 Logins.**

The Last 10 Logins table appears, showing the following information for the last 10 logins.

Field	Description
Login Name	User's login name.
Logged In Since	Date and time the user logged in (GMT).
IP Address	IP address of the system from which the user logged in.
Associated role	Role assigned to the user.

Downloaded from www.Manualslib.com manuals search engine

Related Topic

Overview: Security, page 6-55

Backing Up and Restoring Data

Backing up the WLSE saves its configuration data in case you need to restore the data. When you select **Administration > Appliance > Backup and Restore**, the following options appear:

- **Configure**—Set the backup location (see Specifying the Backup Location, page 6-61).

  Before a Windows 2000 or Windows XP system can be used for backups, it must be configured—see Configuring a Windows 2000 or Windows XP Server as a Backup Location, page 6-62.

- **Backup**—Back up data, including all Wireless LAN Solution Engine role and user information (see Backing Up Data, page 6-63).

- **Restore**—Restore an available backup image (see Restoring Data, page 6-64).

Specifying the Backup Location

The backup location must be running an FTP server, because the Wireless LAN Solution Engine uses FTP to transfer the backup data.

Procedure

Step 1 Select **Administration > Appliance > Backup and Restore > Configure**.

Step 2 Enter the hostname/IP for the backup location.

Step 3 Enter the username you use on the backup location machine.

Step 4 Enter the password you use on the backup location machine.

Step 5 Reenter the password to verify that it is correct.

Step 6 Optional—Specify the path to which the backup image is saved.

When specifying the path on a Windows 2000 or Windows XP server:

- Use either forward slashes (/) or backslashes (\) as the directory separators.

Downloaded from www.Manualslib.com manuals search engine

- Do not include the drive specifier (for example c:\) in the path specification.
- The path is relative to the ftproot.

Step 7 Click **Save**.

Step 8 To verify that the backup location is reachable and is running an FTP server:

a. Select **Administration** > **Appliance** > **Backup and Restore** > **Backup**.

b. Click **Test**.

c. Click **OK**.

Related Topics

- Backing Up Data, page 6-63
- Restoring Data, page 6-64
- Configuring a Windows 2000 or Windows XP Server as a Backup Location, page 6-62

Configuring a Windows 2000 or Windows XP Server as a Backup Location

To serve as a backup location, a Windows 2000 or Windows XP server must be configured for UNIX directory mode.

Procedure

Step 1 On the server, select **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Internet Services Manager**.

If this option is not available on the server, enable it as follows:

a. Select **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.

b. On the left side of the Add/Remove window, click **Add/Remove Windows Components**. The Windows Components wizard starts.

c. Check the checkbox for Internet Information Services, then click **Next**.

Step 2 From the Tree panel, select the Windows 2000 or Windows XP system name.

Step 3 In the Description panel, right-click **Default FTP Server**. Then click **Properties**.

Step 4 In the Home Directory tab:

Downloaded from www.Manualslib.com manuals search engine

- Select **UNIX** under Directory Listing Style.
- Select **Write** under FTP Site Directory.

Backing Up Data

Data backed up includes Wireless LAN Solution Engine role and user information, discovery configuration information, and other configuration information. The following procedure includes a verification step; it is recommended that you always verify that the backup succeeded.

Note You should perform a backup every time you add a user.

Procedure

Step 1 Configure the backup location (see Specifying the Backup Location, page 6-61).

Step 2 Select **Administration** > **Appliance** > **Backup and Restore** > **Backup**.

Step 3 To verify that the backup location is reachable and is running an FTP server:

a. Select **Administration** > **Appliance** > **Backup and Restore** > **Backup**.

b. Click **Test**.

c. Click **OK**.

Step 4 Click **Backup**. The WLSE saves the backup image.

Step 5 To verify that the backup succeeded:

a. Select **Administration** > **Appliance** > **Backup and Restore** > **Restore**.

b. The backup image should be listed in the Available Images list.

c. Click **Cancel**.

You can also log in to the backup location system and verify that there is a backup directory containing *WLSE hostname_date_time*.inf and *WLSE hostname_date_time*.tar files.

Downloaded from www.Manualslib.com manuals search engine

Related Topic

Restoring Data, page 6-64

Restoring Data

Procedure

Step 1 Select **Administration > Appliance > Backup and Restore > Restore**.

Step 2 From the Available Images list, select a backup image. Images are listed by Wireless LAN Solution Engine hostname and date and time of backup.

Step 3 Click **Restore**. The Restore Backup window opens.

Step 4 Click **OK**.

The Wireless LAN Solution Engine shuts down and restarts while data is being restored.

Related Topics

- Backing Up Data, page 6-63
- Specifying the Backup Location, page 6-61

Using Diagnostics

The Diagnostics options are:

- **WLSE Info**—Gather troubleshooting information about the WLSE status and create status reports (see Viewing and Creating a Status Report, page 6-65).
- **Self Test**—Create and display self tests (see Viewing and Creating a Self-Test Report, page 6-65).
- **Processes**—View WLSE process status, stop and start processes (see Viewing Processes, page 6-66).

Downloaded from www.Manualslib.com manuals search engine

Viewing and Creating a Status Report

The WLSE information and status report shows general WLSE status, log files, package information, database status, process status, web server information, Java class information, and log files.

Note Status reports show UTC time.

Procedure

Step 1 Select **Administration > Appliance > Diagnostics > WLSE Info**. The WLSE Information and Status Report dialog box appears.

Step 2 To display a report, click its name. If there are no reports listed, you must create a new report by clicking **Create**.

Step 3 To create a new report, click **Create**. It will take five to seven minutes for the report to be complete. To display the new report, click its name. If the new report is not listed, click **Refresh**.

Step 4 To delete a report, click the report check box, then click **Delete**.

Related Topics

- Viewing and Creating a Self-Test Report, page 6-65
- Viewing Processes, page 6-66

Viewing and Creating a Self-Test Report

Self-tests show the status of WLSE memory, the database, DNS setup, and backup location configuration. Self-test reports indicate whether the tests passed or failed.

Note The self-test shows UTC time.

Downloaded from www.Manualslib.com manuals search engine

Procedure

Step 1 Select **Administration > Appliance > Diagnostics** > **Self Test**. The WLSE Self-Test Report dialog box appears.

Step 2 To display a report, click its name. If there are no reports listed, you must create a new report by clicking **Create**.

Step 3 To display the new report, click its name. If the report is not displayed, click **Refresh**.

Step 4 To delete a report, select the report check box, then click **Delete**.

Related Topics

- Viewing and Creating a Status Report, page 6-65
- Viewing Processes, page 6-66

Viewing Processes

You can view the status of the major processes running on the Wireless LAN Solution Engine using this option. You can also start and stop processes and access complete reports.

Procedure

Step 1 Select **Administration > Appliance > Diagnostics** > **Processes**. The Process Report displays the following:

Column	Description
Process name	Describes how a process is registered. For information on the processes displayed, see Processes Displayed, page 6-68.
State	Process status and a summary of the log file entries for the process.
Pid	Process ID. A unique number by which the operating system identifies each running program.

Downloaded from www.Manualslib.com manuals search engine

Column	Description
RC	Return code. “0” represents normal program operation. Any other number typically represents an error. Refer to the error log.
Signo	Signal number. “0” represents normal program operation. Any other number is the last signal delivered to the program before it terminated.
Start Time	Time (UTC) and date the process was started.
Stop Time	Time (UTC) and date the process was stopped.
Core	The entry “Not applicable” means the program is running normally. The entry “Core file created” means the program is not running normally and the operating system has created a file called a core file. The core file stores important data about processes.
Information	The entry indicates what the process is doing. “Not applicable” means the program is not running normally.

Step 2 Perform any or all of these tasks:

- To view details, click any process name. The Daemon Information window opens. For information on the contents of this window, see Daemon Information, page 6-68.
- To view process status, click any process state. The System Log window opens. For information on the contents of this window, see System Log, page 6-69.
- To stop a process, select the check box next to the process name and click **Stop**. The Process Status table displays the new status and other process information. The WebServer and Tomcat processes cannot be stopped.
- To start a stopped process, select the check box next to that process name and click **Start**. The Process Status table displays the new status and other process information.
- To update the Process Status table with the latest data, click **Refresh**. The table does not automatically update.

Downloaded from www.Manualslib.com manuals search engine

- To see a complete report of all processes running on the WLSE, click **Complete Report**.

Processes Displayed

The Process Status table displays the status of the following major WLSE-specific processes:

Process Name	Description
WLSEjobvm	The job virtual machine.
WLSEFaults	The fault manager.
WebServer	The Web Server.
Tomcat	The Java servlet engine.
ExcepReporter	The process that forwards traps.
CDPbrdcast	The CDP daemon that identifies Cisco devices to their immediate neighbors.
PerfMon	The process that monitors performance.

Daemon Information

The Daemon Information dialog box displays the following:

Field	Description
Process	The process name.
Path	The file location.
Flags	The flags used to register the process with the Daemon Manager.
Startup	The method used to start the process.
Dependencies	The other processes that must be running for this process to run.

Downloaded from www.Manualslib.com manuals search engine

System Log

The system log, which describes the status of the processes running in the system, displays the following:

Field	Description
Timestamp	The date and time the message is logged.
Process	The process that logged the message.
Type	The message type, such as INFO, WARNING, CRITICAL.
Information	The process status as known by the Daemon Manager.

Setting Up the Splash Screen Message

The Splash Screen option allows you to set up a message that is displayed when a user logs in. After viewing the message, the user clicks **Agree** to continue logging in **Disagree** to log out.

Procedure

Step 1 Select **Administration** > **Appliance** > **Splash Screen**. The Splash Screen Message window appears.

Step 2 Enter the message to be displayed.

Step 3 Check the **Enable** check box, then click **Apply**. The splash screen message is enabled.

Note You *must* check **Enable** for the message to appear.

Setting the Current Time and Date on the WLSE

This option allows you to set the current time and date on the WLSE. This time and date appear in WLSE displays.

Downloaded from www.Manualslib.com manuals search engine

To set the UTC time, use the following CLI command:

clock {set *hh***:***mm***:***ss month day year***}**

For more information on this command see the *User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*—From the online help, click **View PDF**.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration** > **Appliance** > **TIME/NTP/NAME**.

Step 2 In the Current Time area, select the new time and date parameters from the lists and click **Update**.

Specifying NTP Time Servers

This option allows you to maintain the current time on the WLSE by using NTP (Network Time Protocol) servers.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration** > **Appliance** > **TIME/NTP/NAME**.

Step 2 To remove an NTP server, select it from the Current Servers list and click Remove.

Step 3 To add an NTP server, enter the server's IP address in the NTP Server IP Address text box and click **Enable**.

Downloaded from www.Manualslib.com manuals search engine

Specifying Name Servers

You can specify the addresses of up to three name servers for name and address resolution.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration** > **Appliance** > **TIME/NTP/NAME**.

Step 2 To remove a name server, select it from the Current Servers list and click **Remove**.

Step 3 To add a name server, enter its IP address in the Name Server IP Address textbox and click **Enable**.

Specifying an SMTP Mail Server

To ensure that WLSE email notifications reach their destinations, you can specify an SMTP mail server. This setting affects email notifications about firmware and configuration jobs, email of reports, and email of fault notifications.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration** > **Appliance** > **Configure Mailroute**.

Step 2 Enter the hostname or IP address of an SMTP mail server on your network and click **Save**.

Downloaded from www.Manualslib.com manuals search engine

Using Connectivity Tools

The options in the Connectivity Tools window allow you to perform connectivity tests and find information about devices.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Appliance > Connectivity Tools**. The Network Connectivity and Security Test dialog box appears.

Step 2 Enter a device name or IP address in the Device text box.

Step 3 Click an option button:

Note Pressing **Enter** will not work. You *must* click a button.

- Ping—Test device reachability.
- Traceroute—Detect routing errors between the Wireless LAN Solution Engine and the target device.
- NSLookup—Look up device or host information via the name server. The information displayed includes server name, server IP address, device name, and the device IP address.
- TCP Port Scan—Find the active ports on the device.
- SNMP Reachable—Try to reach a device by using SNMP. To reach a device using SNMP, the device's credentials must be entered into the SNMP Communities window (select **Administration > Discover > DEVICE CREDENTIALS > SNMP Communities**).

A results window appears, telling you whether the connectivity test was successful.

Step 4 Click **Close** to close the results window.

Downloaded from www.Manualslib.com manuals search engine

Managing System Parameters

The System Parameters window allows you to set certain global parameters. For example, to change the interval at which the Wireless Clients reports will be updated, change the value of the Wireless Client Poll Interval parameter.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration** > **System Parameters**. The following parameters are displayed in the System Parameters window:

Table 6-10 System Parameters

Parameter	Description
Inventory Poll Interval	Interval at which the configuration data will be collected from the devices. (This is the data shown in any GUI device detail table.) **Tip** For more accurate trending, set this parameter at a lower interval than the Inventory Performance Attributes Polling Interval. Default: 1 hour
Wireless Client Poll Interval	Interval at which the device data is collected for client information and at which the Wireless Clients reports are updated. Default: 5 minutes
Inventory Performance Attributes Polling Interval	Interval at which the performance and utilization data will be collected from the devices. To set the aggregation period of this data, change the Aggregation Interval parameter. Default: 15 minutes

Downloaded from www.Manualslib.com manuals search engine

Table 6-10 System Parameters (continued)

Parameter	Description
Aggregation Interval	Interval at which the performance data (from Inventory Performance Attributes Polling Interval) is aggregated. This is the data shown in Report Trends. **Note** For reports it is necessary to compute some attributes over longer periods (average, percentages, changes). This interval determines how often these computations are performed. Default: 3 hours
Short Term Trending Inventory Truncation Interval	How long the performance data (from Inventory Performance Attributes Polling Interval) is retained by the WLSE. Default: 1 day
Aggregation Truncation Interval	How long the aggregated (historical) data is retained by the WLSE. Default: 15 days
Fault History Truncation Interval	How long the fault data is retained. This is the data shown in Fault Description. Default: 30 days
Job History Truncation Interval	How long job data is retained. This is the data shown in **Configure > Jobs**, **Firmware > Jobs**, and **Reports > Scheduled Email Jobs**. **Note** Recurring jobs are truncated every day to retain the last 30 runs. Default: 30 days

Step 2 To change a parameter's interval, select new values from the pulldown lists and click **Apply** to save the changes. To reset the system parameter to their previous values, click **Reset.**

Downloaded from www.Manualslib.com manuals search engine

Note To reset parameters to previous values, click **Reset** before saving.

A confirmation dialog appears. To return to the System Parameters window, click **Back**.

Administering Users

The User Admin options allow you to manage user roles and logins:

- **Manage Roles**—Add, modify, and delete roles (see Managing Roles, page 6-75).
- **Manage Users**—Add, modify, and delete user accounts (see Managing Users, page 6-77).

Related Topic

Modifying Your Profile, page 6-80

Managing Roles

Use this option to add, modify, and delete user-defined roles and to modify predefined roles. A user's role determines the tabs and subtabs the user can access. Users who have access to a subtab can perform all of the tasks under the subtab.

Although you cannot delete predefined roles, you can modify them. The predefined roles and their default privileges are:

- System administrator—Superuser access to the Wireless LAN Solution Engine (can perform any task). The password is the password assigned during initial WLSE setup (using the console). You can change the password using the console or the WLSE's Manage Users option (see Managing Users, page 6-77).
- Network administrator—Monitoring authority, device configuration authority, and discovery configuration authority.
- Network operator—Monitoring and device configuration authority.

Downloaded from www.Manualslib.com manuals search engine

- Help desk—Monitoring authority only.

You can create other roles, which can be modified or deleted.

Note Your login determines whether you can use this option.

Procedure

Step 1 To access the role management window, select **Administration > User Admin > Manage Roles**. Role names are displayed in the center pane. To view the subtabs to which the role has access, select the role.

- The admin user can view all existing roles.
- Other users can only view the roles assigned to them and any roles that they have created.

Step 2 To add a role:

a. Replace the text *New Role* with the name you have chosen for the new role.

b. Select the check boxes next to the features the role will access. Click **Add**.

Note When you select a feature (for example, Display Faults), the role is granted access to the corresponding subtab (for example, **Faults > Display Faults**).

c. The new role appears in the list of roles in the middle pane.

Step 3 To modify a role, select the role. Select the check boxes for the features you want to add to the role and deselect the check boxes next to the features you want to remove from the role. Then click **Modify** to save the changes.

Step 4 To delete a user-defined role, select the role, then click **Delete**.

Related Topics

- Naming Guidelines, page A-1
- Managing Users, page 6-77

Downloaded from www.Manualslib.com manuals search engine

Managing Users

Use this option to:

- Add Users, page 6-77
- Modify Users, page 6-78
- Delete Users, page 6-80

Add Users

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > User Admin > Manage Users**. The Add/Modify/Delete dialog appears. The Users list displays the current users.

- The admin user can view and modify all existing users.
- Other users can view their own logins and any users they have created.

Step 2 Enter the following information, in the order shown:

Note To clear your entries and start over, click **Clear**.

Field	Information to Enter
User Name	Enter the name of the new user.
User Password	Enter a password for new user.
Confirm Password	Reenter the password.
Email	Enter the email address of the user (optional).

Downloaded from www.Manualslib.com manuals search engine

Field	Information to Enter
CLI Access	Select the user's access to the WLSE CLI: None, Level 0, or Level 15. By default, Level 15 is selected for System Administrator, and None is selected for other users. Users with privilege level 15 can use all commands, and users with privilege level 0 can use a subset.
Roles	Select one or more roles for the user. To add a role, select it from the pulldown list. To view a role, select it and click **show role**. To remove a role, select it and click **remove**.

Step 3 To add the new user, click **Add**. The new username appears in the Users list. To discard your changes, click **Clear**.

Modify Users

Note Your login determines whether you can use these options.

Procedure

To modify a user:

Step 1 Select **Administration > User Admin > Add/Modify/Delete**. The Add/Modify/Delete dialog appears. The Users list displays the current users.

Note Only the logins created by you are displayed. If logins were created by another user, they are not visible; only their creator can display them. The admin user can view all logins.

Downloaded from www.Manualslib.com manuals search engine

Step 2 Select the user from the Users list and make the desired changes:

Field	Information to Enter
User Name	Enter the user's name.
User Password	Enter a new password for new user.
Confirm Password	Reenter the new password.
Email	Enter or change the user's email address.
CLI Access	Change the user's access to the WLSE CLI: None, Level 0, or Level 15. By default, Level 15 is selected for System Administrator, and None is selected for others. Users with privilege level 15 can use all commands, and users with privilege level 0 can use a subset. For information on commands available for each privilege level, see the *User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*—From the online help, click **View PDF**.
Roles	Change the user's roles. To add a role, select it from the pulldown list. To view a role, select it and click **show role**. To remove a role, select it and click **remove**.

Step 3 Click **Modify** to save your changes or **Clear** to discard your changes.

Related Topics

- Naming Guidelines, page A-1
- Managing Roles, page 6-75

Downloaded from www.Manualslib.com manuals search engine

Delete Users

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > User Admin > Manage Users**. The Manage Users dialog appears.

Step 2 Select the username from the Users list, then click **Delete**. A confirmation dialog appears. After you click **OK**, the user is deleted.

Modifying Your Profile

Use the My Profile tab to change your password.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > My Profile > Change password**.

Step 2 To change your password, enter a new password in the New Password and Re-enter New Password fields. For information on allowable characters, see Naming Guidelines, page A-1.

Step 3 Click **Apply** to save your changes or **Reset** to discard your changes.

Related Topic

- Modify Users, page 6-78
- Naming Guidelines, page A-1

Downloaded from www.Manualslib.com manuals search engine

Linking to a CiscoWorks2000 Server

You can link to a CiscoWorks2000 server and display the server's desktop in the right pane or in a separate window.

Note This feature is available to all users.

Procedure

Step 1 Select **Administration** > **Links**. The Add Links window and list of links appear.

Step 2 To connect to a CiscoWorks2000 server, click a link in the left pane. The server desktop will appear.

Step 3 To add a link:

d. Enter the name of the link and the URL of the server in the Add Link window; for example: http://cw2k_server:1741.

e. If you want the server desktop to appear in the right pane of the WLSE display, deselect **Open in New Window**. Otherwise, the server desktop opens in a separate window. It is recommended that you allow the server desktop to open in a separate window.

f. Click **Save**. The link is added to the Links list in the left pane.

Step 4 To edit a link, click **Edit** under the name of the link in the Links list. Make your changes and click **Save**.

Step 5 To delete a link, select the link name in the Links list and click **Delete**.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Frequently Asked Questions

Q. What ports and protocols does the WLSE use?

A. For discovery and fault monitoring, the WLSE primarily uses SNMP (UDP port 161). For applying configuration changes, the WLSE uses SNMP, HTTP (TCP port 80 or as configured), and TFTP (UDP port 69).

Q. How do configuration files get transferred to access points?

A. Even though access points support both TFTP and FTP, the WLSE uses only TFTP to upload and download configuration files.

Q. Can you undo a configuration update?

A. Yes, but only after a successful configuration update has taken place.

Q. Is Telnet enabled or disabled by default on the WLSE?

A. Telnet is disabled by default for security reasons.

Q. Can you verify the status of the database?

A. You can verify that the WLSE database is running by using the **show process** CLI command. If the command output includes the db2sync process, the database is running.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Troubleshooting

This section provides suggestions for troubleshooting the Wireless LAN Solution Engine components. If the suggestions do not resolve the error, check the release notes for a possible work around, or contact the Cisco TAC or your customer support.

This section includes troubleshooting suggestions for the following:

- Faults, page 8-2
- Configure, page 8-3
- Firmware, page 8-8
- Reports, page 8-9
- Administration, page 8-11

Downloaded from www.Manualslib.com manuals search engine

Faults

Table 8-1 Troubleshooting Hints for Faults

Feature	Symptom	Probable Cause	Possible Solution
Faults > Display Faults	The Display Fault view is blank.	There are no faults to report based on the filtering criteria you entered.	Not applicable.
	The Description column in the Display Faults table shows, "SNMP query received authentication error response."	The user created for community strings does not have Admin, Ident, Firmware, and SNMP privileges.	Make sure the SNMP community string set on the WLSE (**Administration > Discover > Device Credentials**.) is the same as the string set on the access point (**Setup > Security > User Information)**.
	The Description column in the Display Faults table shows, "Authentication failed. Please check LEAP credentials."	The server is reachable but the credentials are incorrect.	Make sure that the credentials are set correctly by selecting **Administration > Discover > LEAP, RADIUS, or EAP-MD5 Server**.
Faults > Notification Settings	Email fails to arrive at destination.	The SMTP server is not configured properly.	Configure the SMTP server by selecting **Administration > Appliance > Configure Mailroute**.

Downloaded from www.Manualslib.com manuals search engine

Configure

Table 8-2 Troubleshooting Hints for Configure

Feature	Symptom	Probable Cause	Possible Solution
Configure > Templates	The access point is inaccessible through the HTTP port set through template configuration job.	The HTTP port setting does not take effect until the access point is cold restarted.	Cold restart the access point.
	Template configuration job fails every time.	The access point is not set up properly.	Make sure the WLSE is configured as a TFTP server for the access point. For additional information, see Set Up Devices, page 6-12.
Configure > Jobs	The Undo function does not work.	Your job includes custom values.	None.
		Your job includes routing table configurations (only for versions prior to 11.23T).	
		Your job for undoing a user shows as successful but the user is not removed from the access point.	The Undo function only works for new users that are added to the access point. If a user is being added in place of an existing user on the access point, the existing user will remain after the Undo job.

Downloaded from www.Manualslib.com manuals search engine

Table 8-2 Troubleshooting Hints for Configure (continued)

Feature	Symptom	Probable Cause	Possible Solution
		Your job includes the following Security options, which are not supported by the Undo function: • Local Admin Authentication under the Local Admin Access • Encryption Key Values under Local AP/Client Security • Shared Secret under Server-Based Security. • Shared Secret under Accounting.	
		Your job includes the FTP username and password.	
		You are trying to Undo a job that has already been undone.	
		Your job is HTTP-based but you have not set up the HTTP credentials.	Add HTTP credentials using **Administration >Discover >Device Credentials > HTTP User/Password**
		You are trying to Undo a job that contains Custom values, which are not supported by the Undo function.	None.

Downloaded from www.Manualslib.com manuals search engine

Table 8-2 Troubleshooting Hints for Configure (continued)

Feature	Symptom	Probable Cause	Possible Solution
Configure > Jobs	An HTTP job does not run or fails.	The credentials are not set properly.	Make sure the credentials on the WLSE are the same as the credentials on the access point or bridge using **Administration > Discover > Device Credentials**.
			Make sure the credentials on the access point or bridge have firmware rights.
		The TFTP server is not set up correctly.	The TFTP setting on the access point should point to the WLSE as its TFTP server. This can be done by applying a template configuration, containing TFTP server settings, through an SNMP job (only 11.08T and higher)
	The device is not responding to HTTP jobs.	HTTP browsing is disabled on the AP because of this job run.	At the access point console, turn on non-console browsing, or schedule an SNMP job for the device if its version is11.08T or higher.
	An SNMP job does not run or fails.	The community string is not set properly.	Make sure the SNMP community string set on the WLSE is the same as the string set on the access point or bridge using **Administration > Discover > Device Credentials**.
			Make sure the SNMP community string on the access point or bridge has firmware rights.

Downloaded from www.Manualslib.com manuals search engine

Table 8-2 Troubleshooting Hints for Configure (continued)

Feature	Symptom	Probable Cause	Possible Solution
Configure > Jobs	The job failed.	There are multiple reasons a job may have failed.	Make sure all the bootstrapping steps have been performed correctly on the access point.
			Check the jobvm.log by selecting **Administration > Appliance > Status > View Log File** to further identify and report the problem.
		When applying a configuration template on a job with multiple devices, if the job fails on even one of the devices, the job is categorized as Failed.	Check if the **Job Run Detail > Job Run Log** to identify exactly which job(s) failed.
	The job is unverified.	If after applying a configuration template on a device, the device reboots, the job will be categorized as Unverified.	Check the access point to verify whether the job has completed and the new template has been applied.
	The job failed and the **Job Run Detail > Job Run Log** indicates a timeout while reaching the device.	The configuration template you applied has caused the device to either reboot or made it inaccessible.	Make sure the configuration you apply will not cause the device to become inaccessible. For example, do not set up access lists that block all traffic to the Ethernet port. If the device is inaccessible, it might have rebooted after the configuration template was applied. Refer to the template screens to see if any variable is set with an R indicating a possible reboot if the setting is applied.

Downloaded from www.Manualslib.com manuals search engine

Table 8-2 Troubleshooting Hints for Configure (continued)

Feature	Symptom	Probable Cause	Possible Solution
Configure > Jobs	The job is reported as failed, but the configuration was applied successfully to the devices.	The SNMP timeout to the device is too short.	Select **Administration > Discover > Device Credentials > SNMP Communities** and increase the SNMP timeout.
	The job completed with errors.	This error can be seen in jobs where pre- or post-configuration backups before or after applying the new configuration fail, but the new configuration is applied successfully.	Check if "Completed with errors" appears in the **Job Run Detail > Job Run Log** to identify this problem.
	There is a time discrepancy in scheduled jobs.	The time is not set correctly on the WLSE.	1. Reset the WLSE time to Universal Coordinated Time (UTC) using CLI commands as follows: a. Enter **services stop** to stop services. a. Enter the **clock** command to reset the time. a. Enter **services start** to restart the services. 2. Set the time in local browser time, select **Administration > Appliance > Time/NTP/Name**.

Downloaded from www.Manualslib.com manuals search engine

Firmware

Table 8-3 Troubleshooting Hints for Firmware

Feature	Symptom	Probable Cause	Possible Solution
Firmware > Jobs	There is a time discrepancy in scheduled jobs.	The time was not set correctly on the WLSE.	1. Reset the WLSE time to Universal Coordinated Time (UTC) using CLI commands as follows: a. Enter **services stop** to stop services. a. Enter the **clock** command to reset the time. a. Enter **services start** to restart the services. 2. Set the time in local browser time, select **Administration > Appliance > Time/NTP/Name**.
	Firmware is not updated on all the devices included the job.	There were warnings during the job but Ignore Warnings was not set. A firmware job runs even though there are warnings, but the job fails for the devices that had warnings.	Select Ignore Warnings in **Firmware > Jobs > Create Job** before running the job. See Finishing the Job, page 4-14.
	Email about job completion fails to arrive at destination.	The SMTP server is not specified.	Configure the mail route by selecting **Administration > Appliance > Configure Mailroute**. See Specifying an SMTP Mail Server, page 6-71.

Downloaded from www.Manualslib.com manuals search engine

Table 8-3 Troubleshooting Hints for Firmware

Feature	Symptom	Probable Cause	Possible Solution
Firmware > Jobs (continued)	An SNMP job fails	The read community string does not have sufficient permissions.	To allow SNMP reads, the access point mut have a user with at least SNMP and FIRMWARE permissions, and the read community defined on the WLSE must be equivalent to a user on the access point with SNMP and FIRMWARE permissions. For more information, see Set Up Devices, page 6-12 and Specify Community Strings, page 6-7.

Reports

Table 8-4 Troubleshooting Hints for Reports

Feature	Symptom	Probable Cause	Possible Solution
Reports	After running a job, the updated data does not appear in a report.	A full polling cycle has not completed and the new data has not been entered in the database.	Verify that the polling cycle has completed as follows: 1. Select **Administration > Appliance > Status > View Log File**. 2. Click **jobvm.log**. 3. Scroll through the log to find the message: “Finished Inventory” for your particular job.

Downloaded from www.Manualslib.com manuals search engine

Table 8-4 Troubleshooting Hints for Reports (continued)

Feature	Symptom	Probable Cause	Possible Solution
Reports > Scheduled Email Jobs	Email fails to arrive at its destination.	The SMTP server is not configured properly.	Configure the SMTP server by selecting **Administration > Appliance > Configure Mailroute**.
	There is a time discrepancy in the scheduled email jobs.	The time is not set correctly on the WLSE.	1. Reset the WLSE time to Universal Coordinated Time (UTC) using CLI commands as follows: a. Enter **services stop** to stop services. a. Enter the **clock** command to reset the time. a. Enter **services start** to restart the services. 2. Set the time in local browser time, select **Administration > Appliance > Time/NTP/Name**.
Reports > Wireless Clients	The access point data in the Historical Associations report is not accurate.	The wireless client was associated with an access point managed by the WLSE, but it subsequently associated with an access point that was added to the network, but not yet managed by the WLSE.	Verify that the associated access points are in the managed devices folder by selecting Administration > **Discover > Managed Devices > Manage/Unmanage**.

Downloaded from www.Manualslib.com manuals search engine

Table 8-4 Troubleshooting Hints for Reports (continued)

Feature	Symptom	Probable Cause	Possible Solution
Reports > Current > Summary **Reports > Current > Detailed**	The report for access points is empty.	The SNMP user may not have the correct rights assigned.	Open a browser window to the access point, and select **Setup > Security > User Information**. Make sure that the user corresponding to the SNMP community (which is set up in WLSE in **Discovery > Device Credentials**) has been granted rights for the following: Ident, firmware, admin, snmp, and write. If not, click on the user and assign all these rights.
Reports > Current	The report is empty for a group report on a user-defined group.	Reports cannot be displayed for a user-defined group that contains another group.	Display individual reports for the sub-groups or devices within the user-defined group.

Administration

The following table lists troubleshooting hints for **Administration > Discover**.

Table 8-5 Troubleshooting Hints for the Discover Subtab

Feature	Symptom	Probable Cause	Possible Solution
Administration > Discover > Managed Devices	Devices were discovered but are not displayed in the GUI; for example, in Reports.	The devices have not been moved to the Managed state.	Select **Administration > Discover > Managed Devices**. Move the devices from New or Unmanaged to Managed. See Manage Devices, page 6-3.

Downloaded from www.Manualslib.com manuals search engine

Table 8-5 Troubleshooting Hints for the Discover Subtab (continued)

Feature	Symptom	Probable Cause	Possible Solution
Administration > Discover > DISCOVER	There is a time discrepancy in the scheduled discovery jobs.	The local or system time is not set correctly on the WLSE.	1. Reset the WLSE system time (UTC) using CLI commands as follows: a. Enter **services stop** to stop services. a. Enter the **clock** command to reset the time. a. Enter **services start** to restart the services. 2. Set the local browser time. Select **Administration > Appliance > Time/NTP/Name**.

Downloaded from www.Manualslib.com manuals search engine

Table 8-5 Troubleshooting Hints for the Discover Subtab (continued)

Feature	Symptom	Probable Cause	Possible Solution
Administration > **Discover** > **DISCOVER**	Devices are not discovered.	The device is not specified as a seed or the CDP distance is not high enough to reach the device.	Specify the device as a seed or increase the CDP distance so that devices are discovered in **Administration** > **Discover** > **Schedule Discovery** or **Run Discovery Now**. See Managing Device Discovery, page 6-10.
		CDP is not enabled on the device.	Enable CDP on the device; see Set Up Devices, page 6-12. If you are not using CDP, you can import devices from a file or from CiscoWorks2000; see Importing Devices, page 6-28.
		The device is a switch that does not have an access point attache dto it.	Switches are not discovered unless they have an access point attached to them. Discovery can proceed beyond the switch, but the switch itself is not discovered. Make sure a properly configured access point is attached to the switch. See Set Up Devices, page 6-12.
		SNMP is not enabled on the device or SNMP community strings are not entered on the WLSE.	SNMP must be enabled on the device and credentials must be entered on the WLSE. See Set Up Devices, page 6-12 or Specifying Device Credentials, page 6-6.
		SNMP timeouts or retries are set too low.	Reset the timeouts and retries. See Specifying Device Credentials, page 6-6.
		The device is down.	None.
		The device is not supported.	None. See the Supported Devices table for supported devices and software versions.

Downloaded from www.Manualslib.com manuals search engine

The following table lists troubleshooting hints for **Administration > Appliance**.

Table 8-6 Troubleshooting Hints for the Appliance Subtab

Feature	Symptom	Probable Cause	Possible Solution
Administration > Appliance > Security > Authentication Modules	Users cannot log in after failure of the alternative authentication source.	The WLSE falls back to the Local authentication module.	Users can log in using their local passwords.
			The system administrator can log in using the admin log in.
			All users with CLI access can log in using the CLI.

The following table lists troubleshooting hints for **Administration > User Admin**.

Table 8-7 Troubleshooting Hints for the User Admin Subtab

Feature	Symptom	Probable Cause	Possible Solution
Administration > User Admin > Manage Users	Some users are not listed.	Only the creator of a user can view that user's name in the list. The admin user, however, can view all users.	None. For more information, see Managing Users, page 6-77.

Downloaded from www.Manualslib.com manuals search engine

Naming Guidelines

- **Names and Descriptions**—allowable characters for names and descriptions (see Name and Description Allowable Characters, page A-1).
- **Roles and Users**—rules to follow when creating new roles and users (see Roles and User Rules, page A-2).

Name and Description Allowable Characters

Names—no more than 64 characters allowed

Descriptions—no more than 256 characters allowed

Character Description	Example
alphanumeric—upper and lower case	a123b, A123B
space	
exclamation mark	!
number sign	#
percent sign	%
ampersand	&
left and right parenthesis	( )
asterisk	*
plus sign	+
comma	,
hyphen, dash, minus	-

Downloaded from www.Manualslib.com manuals search engine

Character Description	Example
full stop (period)	.
solidus (forward slash)	/
colon	:
semicolon	;
less-than and greater-than signs	< >
equals	=
question mark	?
low line (underscore)	_
left and right square bracket	[ ]
reverse solidus (backward slash)	\
left and right curly bracket	{ }
vertical line	|
tilde	~
dollar sign	$

Roles and User Rules

Type	Rules
User Name	• No more than 32 characters. • Case-sensitive. • Any character from the table above.
User Password	• 5-8 characters. • Case-sensitive. • Any alphanumeric character and an underscore.
Role	• No more than 32 characters. • Case-sensitive. • Any character from the table above.

Downloaded from www.Manualslib.com manuals search engine

Command Reference

This appendix summarizes the Wireless LAN Solution Engine's command line interface (CLI) commands. When you make a configuration change using these commands, the system configuration is updated immediately.

This appendix contains the following sections:

- Using the CLI, page B-2
- CLI Conventions, page B-2
- Command Privileges, page B-2
- Checking Command Syntax, page B-2
- Command History Feature, page B-3
- Help for CLI Commands, page B-3
- Command Summary, page B-4
- Command Description Conventions, page B-9
- Privilege Level 0 Commands, page B-10
- Privilege Level 15 Commands, page B-17
- Maintenance Image Commands, page B-75

Downloaded from www.Manualslib.com manuals search engine

Using the CLI

You can use the CLI by:

- Attaching a console to the WLSE
- Accessing the WLSE using Telnet

CLI Conventions

The command-line interface (CLI) uses the following conventions:

- The key combination **^c** or **Ctrl-c** means hold down the **Ctrl** key while you press the **c** key.
- A string is defined as a non-quoted set of characters.
- Use single-quotes (‘) to surround a series of parameters; do not use double-quotes

Do not confuse the WLSE’s CLI with the IOS CLI. Though they are similar, they are not identical.

Command Privileges

Access to CLI commands is controlled by your user account privilege level. Users with privilege level 15 can use all commands. Users with privilege level 0 can use only a subset of the commands. The command descriptions in this appendix are organized by privilege level. For more information about user accounts and privileges, refer to Administering Users, page 6-75.

Checking Command Syntax

The user interface provides several types of responses to incorrect command entries:

- If you enter a command line that does not contain any valid commands, the system displays `Command not found.`

Downloaded from www.Manualslib.com manuals search engine

- If you enter a valid command but omit required options, the system displays `Incomplete command`.
- If you enter a valid command but provide invalid options or parameters, the system displays `Invalid input`.

In addition, some commands have command-specific error messages that notify you that a command is valid, but that it cannot run correctly.

Command History Feature

The CLI provides a command history feature. To display previously entered commands, press the up arrow key. After pressing the up arrow key, you can press the down arrow key to display the commands in reverse order. To run a command, press the Enter key while the command is displayed on the command line. You can also edit commands before pressing the Enter key.

Help for CLI Commands

You can obtain help using the following methods:

- For a list of all commands and their syntax, type **help** and press **Enter**.
- For help on a specific command, use either of the following methods:
  - Type the command name, a space, **help**; then press **Enter**. For example, **ntp help**.
  - Type **help**, a space, and the command name; then press **Enter**. For example, **help ntp**.

The help contains command usage information and syntax.

Downloaded from www.Manualslib.com manuals search engine

Command Summary

Table B-1 summarizes all commands available on the WLSE. Refer to the full description of commands that you are not familiar with before using them.

Table B-1 Command Summary

Command	Privilege Level	Summary Description	Location of Full Description
auth	15	Enables secure remote authentication.	"auth" section on page B-17
backup	15	Backs up the WLSE.	"backup" section on page B-18
backupconfig	15	Sets the configuration for all backup and restore operations.	"backupconfig" section on page B-19
cdp	15	Configures the Cisco Discovery Protocol (CDP).	"cdp" section on page B-20
clock	15	Sets the WLSE's date and time.	"clock" section on page B-21
df	15	Display the current storage usage on the WLSE.	"df" section on page B-22
erase config	15[1]	Erases the configuration in Flash memory and reload the device.	"erase config" section on page B-23
exit	0	Logs user out of the WLSE.	"exit" section on page B-10
gethostbyname	15	Displays IP address of a known domain name.	"gethostbyname" section on page B-25
fsck	N/A[2]	Checks and repairs the filesystem.	"fsck" section on page B-76
firewall		Implements port filtering on the WLSE.	"firewall" section on page B-24
hostname	15	Changes the system hostname.	"hostname" section on page B-25
import	15	Imports host files, or to maps IP addresses to hostnames.	"import" section on page B-26
install configure	15	Configures the repository that the Wireless LAN Solution Engine uses to install updates.	"install configure" section on page B-27

Downloaded from www.Manualslib.com manuals search engine

Table B-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
install list	15	Lists software updates and images currently available on a configured repository.	"install list" section on page B-28
install update	15	Installs software updates and images from a configured repository.	"install update" section on page B-29
interface	15	Configures an Ethernet interface.	"interface" section on page B-30
ip domain-name	15	Defines a default domain name.	"ip domain-name" section on page B-31
ip name-server	15	Specifies the address of up to three name servers for name and address resolution.	"ip name-server" section on page B-32
listbackup	15	Lists all current backups at the configured site.	"listbackup" section on page B-33
mail	15	Debugs and tests email settings.	"mail" section on page B-34
mailcntrl clear	15	Deletes the maillog, sendqueue, or userqueue.	"mailcntrl clear" section on page B-35
mailcntrl list	15	Lists the size of the userlog, userqueue, or the sendqueue.	"mailcntrl list" section on page B-35
mailroute	15	Forwards email to a specified server.	"mailroute" section on page B-36
nslookup	15	Translates a device name to its IP address or an IP address to its device name.	"nslookup" section on page B-36
ntp server	15	Configures the Network Time Protocol (NTP) and allow the system clock to be synchronized by a time server.	"ntp server" section on page B-37
ping	0	Sends ICMP echo_request packets for diagnosing basic network connectivity.	"ping" section on page B-10
reload	15[1]	Reboots the system.	"reload" section on page B-39

Downloaded from www.Manualslib.com manuals search engine

Table B-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
reinitdb	15	Reinitializes the database.	"reinitdb" section on page B-40
repository	15	Configures the Wireless LAN Solution Engine to be a repository server.	"repository" section on page B-40
repository add	15	Transfers software updates and images from a remote server to the Wireless LAN Solution Engine's local repository.	"repository add" section on page B-41
repository delete	15	Deletes software updates and images on the Wireless LAN Solution Engine's local repository.	"repository delete" section on page B-42
repository list	15	Lists software updates and images on the configured local or remote repository.	"repository list" section on page B-43
repository server	15	Starts, stops, or displays the status of the Wireless LAN Solution Engine's local repository.	"repository server" section on page B-44
restore	15	Restores a backed up configuration.	"restore" section on page B-45
route	15	Adds a route through a gateway device.	"route" section on page B-46
services	15	Lists, starts, or stops management services.	"services" section on page B-46
show anilog	15	Displays the Wireless LAN Solution Engine's ANI log.	"show anilog" section on page B-48
show auth-cli	15	Displays the type of authentication used for secure CLI access.	"show auth-cli" section on page B-49
show auth-http	15	Displays the type of authentication used for secure HTTP access.	"show auth-http" section on page B-49
show backupconfig	15	Displays the current backup and restore configuration.	"show backupconfig" section on page B-50
show bootlog	0	Displays the messages logged during the last system boot.	"show bootlog" section on page B-51

Downloaded from www.Manualslib.com manuals search engine

Table B-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
show cdp neighbor	15	Displays the WLSE's nearest neighbor on the network.,	"show cdp neighbor" section on page B-52
show cdp run	15	Displays the Cisco Discovery Protocol (CDP) configuration.	"show cdp run" section on page B-52
show clock	0	Displays the system date and time in Coordinated Universal Time (UTC).	"show clock" section on page B-11
show collectorlog	15	Displays the Wireless LAN Solution Engine's collector log.	"show collectorlog" section on page B-53
show config	15	Displays the system configuration.	"show config" section on page B-54
show daemonslog	15	Displays the Wireless LAN Solution Engine's daemons log.	"show daemonslog" section on page B-55
show dmgtdlog	15	Displays the Wireless LAN Solution Engine's daemon manager log.	"show dmgtdlog" section on page B-56
show domain-name	0	Displays the system domain name	"show domain-name" section on page B-12
show webaccesslog	15	Displays the Wireless LAN Solution Engine's Web access log.	"show webaccesslog" section on page B-57
show weberrorlog	15	Displays the Wireless LAN Solution Engine's Web error log.	"show weberrorlog" section on page B-58
show websslaccesslog	15	Displays the Wireless LAN Solution Engine's Web SSL log.	"show websslaccesslog" section on page B-59
show import	15	Displays imported host files.	"show import" section on page B-59
show install logs	15	Displays the software updates and images available on the configured repository.	"show install logs" section on page B-60
show interfaces	0	Displays information about the system network interface.	"show interfaces" section on page B-13

Downloaded from www.Manualslib.com manuals search engine

Table B-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
show ipchains	15	Displays the IP chains for the selected interface.	"show ipchains" section on page B-60
show hosts	15	Displays the Wireless LAN Solution Engine's host file.	"show hosts" section on page B-61
show maillog	15	Displays the Wireless LAN Solution Engine's mail log.	"show maillog" section on page B-62
show process	0	Displays information about processes running on the system.	"show process" section on page B-13
show repository	15	Displays the status or the access log of a configured repository.	"show repository" section on page B-63
show route	15	Displays the routes currently configured.	"show route" section on page B-64
show securitylog	15	Displays the Wireless LAN Solution Engine's secure log information.	"show securitylog" section on page B-64
show snmp-server	15	Displays the Wireless LAN Solution Engine's SNMP configuration.	"show snmp-server" section on page B-66
show ssh-version	15	Displays the type of SSH enabled.	"show ssh-version" section on page B-66
show syslog	15	Displays syslog information.	"show syslog" section on page B-67
show tech	15	Displays information necessary for Cisco's Technical Assistance Center to assist you.	"show tech" section on page B-68
show telnetenable	15	Displays the Wireless LAN Solution Engine's Telnet status.	"show telnetenable" section on page B-68
show tomcatlog	15	Displays the Wireless LAN Solution Engine's Tomcat log.	"show tomcatlog" section on page B-69
show version	0	Displays information about the current software on the system.	"show version" section on page B-14

Downloaded from www.Manualslib.com manuals search engine

Table B-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
shutdown	15	Shuts down the system in preparation for powering it off.	"shutdown" section on page B-70
snmp-server	15	Configures an snmp agent.	"snmp-server" section on page B-71
ssh	15	Connects to an external host using SSH	"ssh" section on page B-71
ssh-version	15	Enables Secure Shell (SSH) 1, SSH 2, or both SSH 1 and SSH 2.	"ssh-version" section on page B-72
telnet	15	Telnets to an external host.	"telnet" section on page B-72
telnetenable	15	Configures Telnet access.	"telnetenable" section on page B-73
traceroute	0	Displays the network route to a specified host and identify faulty gateways.	"traceroute" section on page B-15
username	15	Creates a new user account or changes an account's properties.	"username" section on page B-74

1. This command is also available in the maintenance image.
2. This command is available only in the maintenance image.

Command Description Conventions

Command descriptions in this document and in the CLI help system use the following conventions:

- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate optional elements.
- Braces ({ }) indicate a required choice. Braces within square brackets ([{ }]) indicate a required choice within an optional element.
- Boldface indicates commands and keywords that are entered literally as shown.

Downloaded from www.Manualslib.com manuals search engine

- Italics indicate arguments for which you supply values.

Privilege Level 0 Commands

This section describes the privilege level 0 commands.

exit

To log out of the system, use the exit command.

exit

Syntax Description

This command has no arguments or keywords.

Example

The following command logs you out of the system:

```
exit
```

ping

To send ICMP echo_request packets for diagnosing basic network connectivity, use the **ping** command.

ping [**-c** *count*] [**-i** *wait*] [**-s** *packetsize*] [**-n**] {*hostname* | *ip-address*}

Syntax Description

c	Sets the number of echo packets to send.
count	Number of echo packets to send.
i	Sets the amount of time to wait between sending each packet.
wait	Amount of time to wait between sending each packet, in seconds. The default is 1.

Downloaded from www.Manualslib.com manuals search engine

s	Sets the size of each echo packet.
packetsize	The size of each echo packet, in bytes. The default is 56.
hostname	Host name of system to ping.
ip-address	IP address of system to ping.
n	Disables reverse DNS lookup.

Usage Guidelines

To use this command with the *hostname* argument, DNS must be configured on the system. To force the time-out of a nonresponsive host or to eliminate a loop cycle, press **Ctrl-c**.

Example

This command sends 4 echo packets to the host otherhost with a wait time of 5 seconds between each packet:

```
ping -c 4 -i 5 209.165.200.224

PING 209.165.200.224 (209.165.200.224) from 209.165.201.0 : 56(84)
bytes of data.
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=0 ttl=246
time=16.3 ms
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=1 ttl=246
time=2.0 ms
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=2 ttl=246
time=2.1 ms
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=3 ttl=246
time=2.1 ms
```

show clock

To display the system date and time in Coordinated Universal Time (UTC), use the **show clock** command.

show clock

Syntax Description

This command has no arguments or keywords.

Downloaded from www.Manualslib.com manuals search engine

Usage Guidelines

Use the **show clock** command to display the system date and time. For more information about the system time, see the section "Setting System Date and Time" in the *Installation and Configuration Guide for the Cisco 1105 Wireless LAN Solution Engine*.

Example

This command displays the system date and time:

```
show clock
12:43:47 Jun 20 2001
```

Related Commands

clock

ntp server

show domain-name

To display the system domain name, use the **show domain-name** command.

show domain-name

Syntax Description

This command has no arguments or keywords.

Example

This command displays the system domain name:

```
show domain-name
cisco.com
```


Downloaded from www.Manualslib.com manuals search engine

show interfaces

To display information about the system network interface, use the **show interfaces** command.

show interfaces

Syntax Description

This command has no arguments or keywords.

Example

This command displays information about system network interfaces:

```
show interfaces
eth0      Link encap:Ethernet  HWaddr 00:02:B3:35:FD:CC
          inet addr:209.165.200.224 Bcast:209.165.201.0
           Mask:255.255.255.224
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:80309 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22451 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:5 Base address:0xef00 Memory:d0c7e000-d0c7ec40
```

Related Commands

interface

show process

To display information about processes running on the system (including the status of the database), use the **show process** command.

show process [**page**]

Note If the db2sync process is listed, the database is running.

Downloaded from www.Manualslib.com manuals search engine

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.

Example

This command displays information about processes running on the system:

```
show process page
PID  PPID     ELAPSED    SZ                  STARTED TTY  COMMAND
    1     0  4-20:04:35   277 Fri Jun 15 16:54:03 2001 ?    init
    2     1  4-20:04:35     0 Fri Jun 15 16:54:03 2001 ?    kflushd
    3     1  4-20:04:35     0 Fri Jun 15 16:54:03 2001 ?    kupdate
    4     1  4-20:04:35     0 Fri Jun 15 16:54:03 2001 ?    kpiod
    5     1  4-20:04:35     0 Fri Jun 15 16:54:03 2001 ?    kswapd
    6     1  4-20:04:28     0 Fri Jun 15 16:54:10 2001 ?    kreiserfsd
   81     1  4-20:04:25     0 Fri Jun 15 16:54:13 2001 ?    kreiserfsd
   82     1  4-20:04:25     0 Fri Jun 15 16:54:13 2001 ?    kreiserfsd
   83     1  4-20:04:25     0 Fri Jun 15 16:54:13 2001 ?    kreiserfsd
   84     1  4-20:04:25     0 Fri Jun 15 16:54:13 2001 ?    kreiserfsd
   85     1  4-20:04:24     0 Fri Jun 15 16:54:14 2001 ?    kreiserfsd
  199     1  4-20:04:23   290 Fri Jun 15 16:54:15 2001 ?    watchdog
  213     1  4-20:04:23   342 Fri Jun 15 16:54:15 2001 ?    idled
  402     1  4-20:04:17   290 Fri Jun 15 16:54:21 2001 ?    syslogd
  411     1  4-20:04:17   360 Fri Jun 15 16:54:21 2001 ?    klogd
  517     1  4-20:04:15   327 Fri Jun 15 16:54:23 2001 ?    crond
  531     1  4-20:04:15   286 Fri Jun 15 16:54:23 2001 ?    inetd
  540     1  4-20:04:14   585 Fri Jun 15 16:54:24 2001 ?    sshd
  585     1  4-20:04:09   842 Fri Jun 15 16:54:29 2001 ?    dmgtd.lnx
-----------more----------
```

show version

To display information about the current software on the system, use the **show version** command.

show version

Syntax Description

This command has no arguments or keywords.

Downloaded from www.Manualslib.com manuals search engine

Example

This command displays the current software on the system:

```
show version
Copyright (c) 1999-2000 by Cisco Systems, Inc.
Build Version (166) Mon Jun 11 16:56:23 PDT 2001
Uptime: 4 days 20 hours 6 mins
Linux/UID32 version 2.2.16-13bipsec.uid32 (gcc version egcs1
```

traceroute

To display the network route to a specified host and identify faulty gateways, use the **traceroute** command.

traceroute [-f *first_ttl***] [-m** *max_ttl***] [-w** *waittime***]** *host* **[***packetlength***]**

Syntax Description

-f	(Optional) Sets the time-to-live used in the first outgoing probe packet.
first_ttl	Time-to-live value of the first outgoing probe packet. The default is 1 hop.
-m	(Optional) Sets the maximum time-to-live (maximum number of hops) used in outgoing probe packets.
max_ttl	Maximum time-to-live for outgoing probe packets. The default is 30 hops.
-w	(Optional) Sets the time to wait for a response to a probe, in seconds.
waittime	Time to wait for a response to a probe, in seconds. The default is 5.
host	Name or IP address of host to which to connect.
packetlength	(Optional) The length of the packet to send, in bytes. The default and minimum value is 40.

Downloaded from www.Manualslib.com manuals search engine

Usage Guidelines

Use the **traceroute** command to trace the network route to a specified host and identify faulty gateways. The command displays a list of the hosts that receive probe packets as they travel to the destination host, in the order that the receiving hosts receive the packets. Asterisks (*) appear as the list entry for hosts that do not respond to probing correctly.

Example

This command displays the network route to the host otherhost with a packet time-to-live value of 2, a wait time of 5 seconds, and 50-byte packets:

```
traceroute -m 20 -w 10 cisco.com 50
traceroute to example.com (209.165.200.224), 20 hops max, 50 byte
packets
 1  ex1.com (209.165.200.225)  0.981 ms  0.919 ms  0.926 ms
 2  ex2.com (209.165.200.254)  1.528 ms  0.747 ms 0.661 ms
 3  ex3.com (209.165.200.255)  0.887 ms  0.770 ms  0.744 ms
 4  ex4.com (209.165.201.0)  0.932 ms  0.789 ms  0.679 ms
 5  ex5.com (209.165.201.1)  1.066 ms  1.052 ms  0.983 ms
 6  ex6.com (209.165.201.30)  1.472 ms  1.247 ms  1.847 ms
 7  ex7.com(209.165.201.31)  1.738 ms  1.424 ms  1.658 ms
 8  ex8.com (209.165.202.128)  3.728 ms  2.429 ms  2.804 ms
 9  ex9.com (209.165.202.129)  6.283 ms  5.499 ms 3.285 ms
10  ex10.com (209.165.202.158)  9.926 ms  73.463 ms  3.895 ms
11  ex11.com (209.165.202.159)  70.967 ms *  47.106 ms
```

Related Commands

ping

Downloaded from www.Manualslib.com manuals search engine

Privilege Level 15 Commands

This section describes the privilege level 15 commands. Only users with privilege level 15 can run these commands.

auth

Use the **auth** command to enable secure remote authentication.

auth {cli | http} {local | tacacs *secret server1* **[***server2***] | radius** *secret server1* **[***server2***] | nt** *domain pdc* **[***bdc***]}**

Syntax Description

cli	Enables authentication using the Command Line Interface (CLI).
http	Enables authentication using Hypertext Transfer Protocol (HTTP).
local	Enables local authentication.
tacacs	Enables authentication using the Terminal Access Controller Access Control System (TACACS).
radius	Enables authentication using Remote Dial-In User Service (RADIUS).
nt	Enables authentication from an NT domain controller.
secret	Shared secret code of server.
server1	IP address or device name of server from which authentication will occur.
server2	IP address or device name of optional secondary server from which authentication could occur
domain	NT domain name.
pdc	Name of the Primary Domain Controller (PDC).
bdc	Name of the Backup Domain Controller (BDC).

Downloaded from www.Manualslib.com manuals search engine

Example

This command enables secure remote authentication from a remote server, using TACACS.

```
auth http tacacs tr5e43 209.165.200.224
```

backup

Use the **backup** command to back upthe WLSE.

backup [test]

Syntax Description

test	Tests the configured backup hostname, username, password, and directory.

Usage Guidelines

To back up the WLSE, use the **backup** command. To configure the backup location, use the **backupconfig** command.

Example

The following command backs up the WLSE:

```
backup
```

Related Commands

backupconfig

listbackup

restore

show backupconfig

Downloaded from www.Manualslib.com manuals search engine

backupconfig

Use the **backupconfig** command to set the configuration for all backup and restore operations. To clear the backup and restore configuration information, use the **no backupconfig** command.

backupconfig {*hostname***} {***username***} {***password***} [***directory***]**

no backupconfig

Syntax Description

hostname	Host name or IP address of the host system.
username	Username of host system.
password	Password of the host system.
directory	Path to specific backup directory, if different from user's default directory.

Usage guidelines

To set the configuration for all backup and restore operations, use the **backup** command.

Example

The following command will configure the backup and restore operations to backup to and restore from host 209.165.200.224, set the username to user1, and set the password to pass:

```
backupconfig 209.165.200.224 user1 pass
```

The following command clears all backup and restore configuration information:

```
no backupconfig
```

Related Commands

backup

listbackup

restore

Downloaded from www.Manualslib.com manuals search engine

show backupconfig

cdp

Use the **cdp** command to configure the Cisco Discovery Protocol

cdp {run [*port***] | timer** *seconds* **| holdtime** *seconds***}**

no cdp {run [*port***] | timer | holdtime}**

Syntax Description

run	start cdp
timer	set cdp packets retransmission time.
holdtime	set cdp packet info hold time.
port	Ethernet port on which CDP will be enabled. Acceptable values are eth0-15.
seconds	amount of time, in seconds, that the system takes to either transmit the cdp packet information or to hold another system's cdp packet information.

Usage Guidelines

Cisco Discovery Protocol (CDP) is a protocol by which one Cisco device can recognize, and be recognized by, another Cisco device. The run command starts the system sending out signals to the other systems. The timer command sets the amount of time, in seconds, that these signals are sent. The holdtime sets the amount of time a system will recognize another system without receiving a signal. For example, if your system's holdtime is set to 30 seconds, and another system that has already been recognized by yours does not send a signal within that 30 seconds, your system will cease to recognize it. If you are using the **no cdp** command, the timer and holdtime commands set their respective values to the default value.

Example

This command sets the cdp packet's retransmission time at 10 seconds.

Downloaded from www.Manualslib.com manuals search engine

```
cdp timer 10
```

This command sets the cdp packet's retransmission to its default time.

```
no cdp timer
```

clock

To set the system date and time, use the **clock** command. See the Usage Guidelines before using this command.

clock {set *hh***:***mm***:***ss month day year***}**

Syntax Description

set	Sets the system clock.
*hh***:***mm***:***ss*	Current time (for example, 13:32:00).
month	Current month. You can enter full month names or abbreviations that include at least the first 3 characters of the month name (for example, jan, feb, mar).
day	Day of the month (for example, 1 to 31).
year	Current year (for example, 2000).

Usage Guidelines

When resetting the time, you must stop and restart WLSE services. Otherwise, scheduled configuration and firmware jobs will not run properly. To reset the time:

Step 1 Stop services:

```
services stop
```

Step 2 Change the time.

Step 3 Start services:

```
services start
```


Downloaded from www.Manualslib.com manuals search engine

To set the date and time, use the **set** option.

If you configure the system to use Network Time Protocol (NTP), you do not need to set the system clock manually using the **clock** command.When setting the clock, enter the current time in Coordinated Universal Time (UTC).

For more information about the system time, refer to "Setting System Date and Time" in the *Installation and Configuration Guide for the Cisco 1105 Wireless LAN Solution Engine*.

Example

This command sets the date and time:

```
clock set 16:00:00 dec 11 2001

Tue Dec 11 16:00:00 UTC 2001
```

Related Commands

ntp server

s**how clock**

df

To display the current storage usage on the WLSE, use the **df** command.

df

Usage Guidelines

This command in primarily intended as a debugging tool for problems with full partitions.

Example

The following command displays the current storage usage on the WLSE:

```
df
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda12            151M   59M   92M  39% /
/dev/sda1              49M  2.8M   44M   6% /boot
/dev/sda7             985M   24M  911M   3% /extra
```


Downloaded from www.Manualslib.com manuals search engine

```
/dev/sda8              601M   32M  569M   5% /home
/dev/sda6             1001M  136M  865M  14% /opt
/dev/sda13             9.7G   32M  9.7G   0% /tftpboot
/dev/sda9              601M   32M  569M   5% /tmp
/dev/sda10             591M  212M  350M  38% /usr
/dev/sda5              2.9G  450M  2.5G  15% /var
```

erase config

To erase the configuration in flash memory and reload the software, use the **erase config** command.

erase config

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to erase the configuration in flash memory and reload the WLSE software.

When you enter the command, you are prompted for confirmation. Enter **yes** to confirm, or press **Enter** to accept the default response **no**.

Caution When you confirm this command, the system configuration is erased and the system reboots automatically. The system will not operate until you reconfigure it.

When the system reboots, you must reconfigure it with the setup program. For information about using the setup program, refer to the *Installation and Configuration Guide for the Cisco 1105 Wireless LAN Solution Engine*.

Example

This command erases the system configuration:

```
erase config
This will erase your configuration, return device t
o factory defaults, and reload the device
```


Downloaded from www.Manualslib.com manuals search engine

```
Do you want to continue?[no]:yes
```

firewall

To implement port filtering on the WLSE, use the **firewall** command.

firewall *eth <0-5>* **[public | private] | [icmp telnet ssh snmp https 1741]**

Syntax Description

eth <0-5>	Port to be configured. Acceptable values are eth0-5.
public	Denies access via ICMP, Telnet, SNMP, and the HTTP 1741 port.
private	Denies no access.
icmp	Denies Internet Control Message Protocol (ICMP) ping messages.
telnet	Denies incoming Telnet connections.
ssh	Denies incoming SSH connections.
snmp	Denies incoming SNMP requests.
https	Denies all connections to the SSL HTTP port.
1741	Denies all connections to the HTTP 1741 port.

Usage Guidelines

Use the firewall command to implement port filtering on the WLSE. To configure an Ethernet port for secured public access, use the **public** option. To configure an Ethernet port for local access, via a LAN or VLAN, use the **private** option. To *dissable* icmp, Telnet, ssh, snmp, https, or to deny connections to the SSL HTTP port or the HTTP 1741 port, use its corresponding option.

Examples

- Ethernet 0 port is connected to the Internet, and is configured to be accessible only via HTTPS by entering the following command:

  firewall eth0 public ssh 1741

Downloaded from www.Manualslib.com manuals search engine

- Ethernet 1 port is connected to an internal LAN or VLAN, and is configured to be accessible via any of the supported protocols by entering the following command:

  ```
  firewall eth1 private
  ```

  An on-site user has full access to the WLSE, but an external user can only access it using a secure connection.

gethostbyname

Use the gethostbyname command to display the IP address of a known domain name.

gethostbyname *host*

Syntax Description

host	Domain name of host.

Example

This command displays the IP address of example.com

```
gethostbyname example.com
209.165.200.224
```

hostname

To change the system hostname, use the **hostname** command.

hostname *name*

Syntax Description

name	New hostname for the WLSE; the name is case sensitive and may be from 1 to 22 alphanumeric characters.

Downloaded from www.Manualslib.com manuals search engine

Example

The following example changes the hostname to sandbox:

```
hostname sandbox
```

import

To import host files, or to map IP addresses to hostnames, use the **import** command:

import {host *hostname ipaddress***} | {hosts** *ftp-host username password path***}**

no import {host *hostname ipaddress***} | {hosts}**

Syntax Description

host	Maps one IP address to a hostname.
hostname	Hostname to map IP address to.
hosts	Imports host files from ftp accessible host.
ipaddress	IP address to map Hostname to.
password	Password used to access ftp accessible host.
path	Path to ftp accessible host.
ftp-host	IP address of ftp accessible host.
username	username use to access ftp accessible host.

Usage Guidelines

To map a single hostname to an IP address, enter the import command as follows

import host *hostname ipaddress*

To import host files from an external, ftp accessible server, enter the import command as follows:

import hosts *ftp-host username password path*

To remove an individual IP address from a host file, use the **no** version of the **import** command as follows:

Downloaded from www.Manualslib.com manuals search engine

no import host *hostname ipaddress*

To remove an imported host file, use the **no** version of the **import** command as follows:

no import hosts

Example

This command imports host files from the ftp accessible server ftpserver_1. Ftpserver_1 has the username admin, the password pass, and the path /ftpserver_1/hosts.

```
import hosts ftpserver_1 admin pass /ftpserver_1/hosts
```

This command deletes the hosts imported in the example above:

```
no import hosts
```

install configure

To define the repository that the Wireless LAN Solution Engine uses to install software updates and images, use the **install configur**e command.

install configure {URL *URL Value* **| default | save}**

Syntax Description

URL	Sets the URL of the repository.
URL Value	The URL of the repository. The URL should take the form of http://host:port/path (the path is not a requirement).
default	Configures the Wireless LAN Solution Engine to be its own repository. The URL is http://localhost:9851.
save	Saves the current configuration in the install.ini file.

Usage Guidelines

The **install configure** command defines the repository that the Wireless LAN Solution Engine uses. A repository is a remote or local server from where a system can download software updates and images. Only HTTP is supported.

Downloaded from www.Manualslib.com manuals search engine

Example

The following command configures the Wireless LAN Solution Engine to use http://209.165.200.22, with port 9851, as a repository:

```
install configure URL http://209.165.200.224:9851
```

Related Commands

install update

install list

install list

To list software updates and images currently available on the configured repository, use the **install list** command.

install list [all | full | page | updates]

Syntax Description

all	Displays all software updates and images on a configured repository. This command displays the name, the version, the requirements, the type, and a summary of the software.
full	Displays only the complete images on a configured repository.This command displays the name, the version, the requirements, the type, and a summary of the image.
page	Displays only the names of all software updates and images on a configured repository. All other information is omitted.
updates	Displays only the updates on a configured repository. This command displays the name, the version, the requirements, the type, and a summary of the update.

Usage Guidelines

The **install list** command displays software updates and images currently available on a repository. A repository is a remote or local server from where a system can receive software.

Downloaded from www.Manualslib.com manuals search engine

Example

Enter the following command to display a list of all available software updates and images on a configured repository:

```
install list all
Name            Version Requires        Type       Summary
 EX-1.02        1.02    HSE-1.0         UPDATE     Hosting Solution...
 EX-1.1aR       1.1aR   HSE-1.1         UPDATE     Hosting Solution...
 EX-1.1a        1.1a    HSE-1.1         UPDATE     Hosting Solution...
 EX-1.0a        1.0a    HSE-1.0         UPDATE     Hosting Solution...
 EX-1.0aR       1.0aR   HSE-1.0         UPDATE     Hosting Solution...
 EX-1.0-ROB     1.0     HSE-1.0         COMPLETE   Hosting Solution...
 EX-1.0         1.0     HSE-1.0         COMPLETE   Hosting Solution...
```

Related Commands

install configure

install update

install update

To install a software update or image, use the **install update** command.

install update *package name*

Syntax Description

Package Name	Name of the software update or image to be installed. To see the names of software updates and images available for installation, use the **install list** command. For more information, see the "install list" section on page B-28.

Example

The following command installs the update EX-2.0:

```
install update EX-2.0
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

install configure

install list

interface

To configure an Ethernet interface, use the **interface** command.

interface *eth<0-5>* **{[up | down] |** *ipaddress netmask* **[default-gateway** *address***] [up | down]}**

Syntax Description

eth<0-5>	Name of the interface port to be configured. Acceptable values are eth0-5.
up	Enables the interface (the default). If you include the *ipaddress* parameter and want to enable the interface in the same command, either enter the **up** parameter after *ipaddress* and its required parameters, or do not specify the **up** or **down** parameters (**up** is the default).
down	Disables the interface. If you include the *ipaddress* parameter and want to disable the interface in the same command, enter the **down** parameter after *ipaddress* and its required parameters.
ipaddress	The IP address of the interface.
netmask	The netmask of the interface IP address.
default-gateway	Changes the IP address of the default gateway that connects the WLSE to the network.
address	The gateway IP address.

Default

When you enter the **interface** command, the interface that you specify is enabled by default. If you want to disable an enabled interface or leave a disabled interface disabled, you must specify the **down** option.

Downloaded from www.Manualslib.com manuals search engine

Usage Guidelines

Use the **interface** command to configure an Ethernet interface.

If you change the IP address or hostname, follow these steps to ensure that applications using the system can connect to it correctly:

Step 1 Stop and restart management services by entering:

```
# services stop

# services start
```

Step 2 Verify that management applications that use the system can still connect to it.

Step 3 Reconnect any applications that cannot connect to it using the system's new IP address or hostname.

Example

This command disables the Ethernet 1 interface:

```
interface eth1 down
```

This command sets the Ethernet 0 IP address, netmask, and gateway IP address:

```
interface eth0 209.165.200.224 255.255.255.224 default-gateway
209.165.201.31 up
```

ip domain-name

To define a default domain name, use the **ip domain-name** command. To remove the default domain name, use the **no** form of the command.

ip domain-name *name*

no ip domain-name *name*

Syntax Description

name	Domain name (e.g. cisco.com).

Downloaded from www.Manualslib.com manuals search engine

Usage Guidelines

Use this command to define a default domain name.

A default domain name allows the system to resolve any unqualified host names. Any IP hostname that does not contain a domain name will have the configured domain name appended to it. If you are using a DNS server, this appended name is resolved by the DNS server, and then added to the host table.

Example

This command defines the default domain name cisco.com:

```
ip domain-name cisco.com
```

This command removes the default domain name:

```
no ip domain-name
```

Related Commands

ip name-server

ip name-server

To specify the addresses of up to three name servers for name and address resolution, use the **ip name-server** command. To remove a name server, use the **no** form of the command.

ip name-server *ip-address*

no ip name-server *ip-address*

Syntax Description

ip-address	Name server IP address (maximum of 3).

Usage Guidelines

Use the **ip name-server** command to point the system to a specific DNS server. You may configure up to three servers.

Downloaded from www.Manualslib.com manuals search engine

If you attempt to configure a fourth name server, the following error message appears:

```
# Name-server table is full.
```

The system must have a functional DNS server configured to function correctly. If it does not, in most cases it will not correctly process requests from management applications that use it. If the system cannot obtain DNS services from the network, Telnet connections to the system will fail or Telnet interaction with the system will become extremely slow.

Example

This command assigns a name server for the system to use for DNS name to address resolution:

```
ip name-server 209.165.200.224
```

This command disables the name server; the system will not use it for name to address resolution:

```
no ip name-server 209.165.200.224
```

Related Commands

ip domain-name

listbackup

Use the **listbackup** command to list all current backups at the configured site.

listbackup

Syntax Description

This command has no arguments or keywords.

Example

The following command lists all current backups at the configured site:

```
listbackup
```


Downloaded from www.Manualslib.com manuals search engine

```
ex1_06042001_170640: Hostname: ex1 Date: 06042001  time: 1700
ex1_06052001_124543: Hostname: ex1 Date: 06052001  time: 1243
ex1_06052001_155148: Hostname: ex1 Date: 06052001  time: 1558
ex1_06202001_145704: Hostname: ex1 Date: 06202001  time: 1454
```

Related Commands

backup

backupconfig

restore

show backupconfig

mail

To debug and test email settings, use the **mail** command.

mail [to *user@host* **[debug]]**

Usage Guidelines

Entering the **mail** command with no arguments will allow you to read email. Entering the **mail** command with the arguments listed will allow you to send email.

Syntax Description

to	Sends email to the expressed recipient.
user@host	Recipient of the email.
debug	Debugs any email problems.

Example

The following command sends an email message:

```
mail to operator@sj_wlse
Subject: test
This is a test mail
.
Cc:
```


Downloaded from www.Manualslib.com manuals search engine

Note You must end the mail message with a period (.) on a line by itself.

mailcntrl clear

To delete the maillog, sendqueue, or userqueue, use the **mailcntrl clear** command.

mailcntrl clear {log | sendqueue | userqueue}

Syntax Description

log	Clears the WLSE's email log.
sendqueue	Clears the WLSE's sendqueue.
userqueue	Clears the WLSE's userqueue.

Example

The following command clears the WLSE's email log.

```
mailcntrl clear log
```

Related Commands

mailcntrl list

mailcntrl list

To list the size of the userlog, userqueue, or the sendqueue, use the **mailcntrl list** command.

mailcntrl list {logsize | sendqueuesize | userqueuesize}

Syntax Description

logsize	Size of the mail log.
sendqueuesize	Size of the sendqueue.

Downloaded from www.Manualslib.com manuals search engine

userqueuesize Size of the userqueue.

Example

The following command displays the size of the WLSE's email log.

```
mailcntrl list logsize
Mail log files total size: 4.0k
```

Related Commands

mailcntrl clear

mailroute

To forward email to a specified SMTP server, use the **mailroute** command to specify the server. If no server is specified, the WLSE will use DNS to resolve the correct email server in your local domain. To stop forwarding mail to the SMTP server, use the **mailroute** command followed by a blank space.

mailroute {*hostname* | *ip-address***}**

Syntax Description

hostname	Host name of an email server.
ip-address	IP address of an email server.

Example

The following command forwards email to a server with the hostname mailserver:

```
mailroute mailserver
```

nslookup

To translate a device name to its IP address or an IP address to its device name, use the **nslookup** command.

nslookup {*dns-name* | *ip-address***}**

Downloaded from www.Manualslib.com manuals search engine

Syntax Description

dns-name	Device name of a host on the network.
ip-address	IP address of a host on the network.

Example

The following command translates the device name hostname to its IP address:

```
nslookup hostname
Server: dns.ex1.com
Address: 209.165.200.224

Name:    ex1.com
Address: 209.165.201.0
```

ntp server

To configure the Network Time Protocol (NTP) and allow the system clock to be synchronized by a time server, use the **ntp server** command. To disable this function, use the **no** form of this command.

ntp server *ip-address*

no ntp server *ip-address*

Syntax Description

ip-address	IP address of the NTP time server providing clock synchronization.

Usage Guidelines

Use the **ntp server** command to synchronize the system clock with the specified NTP server. If you configure multiple NTP servers, the system will synchronize with the first working NTP server it finds. There is no limit to the number of NTP servers that you can configure.

The **ntp server** command validates the NTP server that you specify. The possible results are:

- If the server is a valid NTP server, a message similar to the following appears:

Downloaded from www.Manualslib.com manuals search engine

```
# 19 Jan 00:43:48 ntpdate[1437]: step time server 209.165.200.224
offset 999.257304
```

- If no NTP server with the name or IP address you specified exists, a message similar to the following appears:

  ```
  # 19 Jan 00:43:40 ntpdate[1431]: no server suitable for
  synchronization found
  ```

  In this case, remove the NTP server by using the **no** form of the command, then configure a valid NTP server.

- If the system time is set to a time later than the time on the NTP server, a message similar to the following appears:

  ```
  # 19 Jan 00:43:58 ntpdate[1265]: Can't adjust the time of day:
  Invalid argument.
  ```

  In this case, the **ntp server** command is entered into the system configuration, but NTP will not function. Follow these steps to remove the command and configure NTP correctly:

Step 1 Remove the **ntp server** command from the configuration by entering the **no** form of the command. For example:

no ntp server *ip-address*

where *ip-address* is the IP address of the NTP server.

Step 2 Set the system clock to a time that is behind the time on the NTP server using the **clock set** command. For more information about the clock command, refer to the "clock" section on page B-21.

Step 3 Enter the **ntp server** command again to configure the NTP server on the system. For example:

ntp server *ip-address*

Example

This command configures the system to use an NTP server:

```
ntp server 209.165.201.0
```


Downloaded from www.Manualslib.com manuals search engine

This command configures the system to stop using the NTP server:

```
no ntp server 209.165.201.0
```

Related Commands

clock

reload

To reboot the system, use the **reload** command.

reload

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use the **reload** command to reboot the system.

You are prompted to verify the reload. Enter **yes** to confirm or **no** to cancel the reload.

Caution All processes running on the system stop when you run the reload command. The WLSE will not respond while it is reloading.

Example

This command reboots the system:

```
reload
```

Related Commands

shutdown

Downloaded from www.Manualslib.com manuals search engine

reinitdb

To reinitialize the database, use the **reinitdb** command.

reinitdb

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

The **reinitdb** command reinitializes the database. This erases all information contained within the database.

Example

This command reinitializes the database:

```
reinitdb
```

repository

To configure the Wireless LAN Solution Engine to be a repository server, use the **repository** command.

repository source *URL*

Syntax Description

source	Sets the location from where the local repository downloads software updates and images.
URL	The IP address of an external server containing software updates and images.

Downloaded from www.Manualslib.com manuals search engine

Usage Guidelines

The **repository** command allows the Wireless LAN Solution Engine to be a repository both for itself and for external systems. A repository is a remote or local server from where a system can receive software updates and images.

The **repository** command only configures the Wireless LAN Solution Engine to be a repository. To configure the Wireless LAN Solution Engine to install software updates and images from this repository, see the "install configure" section on page B-27.

Example

To configure the Wireless LAN Solution Engine to be a repository, and to download software updates and images from http:// 209.165.200.224, enter the following command:

```
repository source ftp://209.165.200.224
```

Related Commands

repository add

repository delete

repository list

repository server

repository add

To transfer software updates and images from a remote server to the Wireless LAN Solution Engine's local repository, use the **repository add** command.

repository add *package*

Syntax Description

package	Name of the software update or image to be transferred.

Downloaded from www.Manualslib.com manuals search engine

Usage Guidelines

The **repository add** command transfers software updates and images from a remote server to the Wireless LAN Solution Engine's local repository. You will be prompted to enter a username and password if they are needed to access the remote server.

Example

To transfer the update EX_2.0 from an update server to the local repository, enter the following command:

```
repository add ex_2.0
```

Related Commands

repository

repository delete

repository list

repository server

repository delete

To delete software updates and images on the Wireless LAN Solution Engine's local repository, use the **repository delete** command.

repository delete [*package* **| all]**

Syntax Description

all	Deletes all software updates and images in the local repository.
package	Name of the software update or image to be deleted.

Downloaded from www.Manualslib.com manuals search engine

Usage Guidelines

The **repository delete** command deletes software updates and images on the Wireless LAN Solution Engine's local repository. A repository is a remote or local server from where a system can receive software updates and images.

Example

The following command deletes the update EX_2.0 from the local repository:

```
repository delete EX_2.0
```

Related Commands

repository

repository add

repository list

repository server

repository list

To list software updates and images on the configured local or remote repository, use the **repository list** command.

repository list {local | remote} [detail] [page]

Syntax Description

local	Lists software updates and packages on the local repository.
remote	Lists software updates and packages on a remote repository.
detail	Includes details of the software updates and images displayed.
page	Displays the software updates and packages on page at a time.

Downloaded from www.Manualslib.com manuals search engine

Example

To list the software updates and images available on the configured local repository, with details and one page at a time, enter the following command:

```
repository list local detail page
```

Related Commands

repository

repository add

repository delete

repository server

repository server

To start, stop, or view the status of the Wireless LAN Solution Engine's local repository, use the **repository server** command.

repository server [stop | start | status]

Syntax Description

stop	Stops the local repository.
start	Starts the local repository.
Status	Displays the status of the local repository.

Usage Guidelines

The **repository server** command starts, stops, or displays the status of the Wireless LAN Solution Engine's local repository. A repository is a remote or local server from where a system can receive software updates and images.

Example

The following command stops the local repository:

```
repository server stop
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

repository

repository add

repository delete

repository list

restore

Use the **restore** command to restore a backed up configuration of the WLSE.

restore *restore name*

Syntax Description

restore name	Name of backup to be used to restore the WLSE.

Usage Guidelines

To restore a configuration, use the **restore** command. If you use the **restore** command all current domains, roles, users, and discovery configuration information will be erased.

Example

The following command will restore a backed up configuration:

```
restore backup1
```

Releated Commands

backup

backupconfig

listbackup

show backupconfig

Downloaded from www.Manualslib.com manuals search engine

route

To add a route through a gateway device, use the **route** command. To delete a route, use the no version of the command.

route {*network address***} netmask {***network netmask***} gateway {***gateway address***}**

no route {*network address***} netmask {***network netmask***}**

Syntax Description

netmask	Sets value of the network netmask.
gateway	Sets the IP address of the router or gateway.
network address	IP address of the network.
network netmask	Value of the network netmask.
gateway address	IP address of router or gateway.

Example

The following command adds a route:

```
route 209.165.201.0 netmask 255.255.255.224 gateway 209.165.200.224
```

The following command deletes the above route:

```
no route 209.165.201.0 netmask 255.255.255.224
```

services

To list, start, or stop the management services running on the system, use the **services** command.

services [status | start | stop]

Downloaded from www.Manualslib.com manuals search engine

Syntax Description

status	Displays the management services status.
start	Starts the management services.
stop	Stops the management services.

Usage Guidelines

Use this command to start, stop, or view status of the management services running on the system.

Management services are the software installed on the system by network management applications. Use this command to stop and restart the management services if the system is not responding correctly to a management application. This should cause the services to reset and function properly again.

Example

This command stops management services:

```
services stop
```

This command starts management services:

```
services start
```

This command shows services status:

```
# services status
Process= HSECollector
        State  = Running but busy flag set
        Pid    = 588
        RC     = 0
        Signo  = 0
        Start  = 06/15/01 16:54:32
        Stop   = Not applicable
        Core   = Not applicable
        Info   = HSECollector started.

        Process= HSEANIServer
        State  = Running but busy flag set
        Pid    = 589
        RC     = 0
        Signo  = 0
        Start  = 06/15/01 16:54:32
-----------more-----------
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

show process

show anilog

To display the Wireless LAN Solution Engine's ANI log, use the **show anilog** command.

show anilog [page] | include *MatchString1* **[***MatchString2***]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's ANI log, one page at a time:

```
show anilog page
/var/adm/CSCOets/log/ani.log
SNMPThrPool: Instantiated ex.lib.snmp.lib.timer.DynamicThreadPool,  mi
n=15, max=48, maxIdleSecs=240
2001/12/20 13:43:12 main ani MESSAGE DBConnection: Created new
Database connecti
on [hashCode = 45981573]
2001/12/20 13:43:38 main ani MESSAGE ServletServiceModule: Moxie
Servlet Engine
is ready to receive requests
2001/12/20 15:43:39 HSEStatusPoll ani MESSAGE DBConnection: Created
new Database
 connection [hashCode = 85057415]
```


Downloaded from www.Manualslib.com manuals search engine

```
2001/12/20 17:43:39 HSEStatusPoll ani MESSAGE DBConnection: Created
new Database
 connection [hashCode = 396959623]
2001/12/20 19:43:39 HSEStatusPoll ani MESSAGE DBConnection: Created
new Database
--More--
```

show auth-cli

To display the type of authentication used for secure CLI access, use the **show auth-cli** command.

show auth-cli

Syntax Description

This command has no arguments or keywords.

Example

This command and response shows that the WLSE's local authentication is being used for the CLI:

```
show auth-cli
local
```

show auth-http

To display the type of authentication used for secure HTTP access, use the **show auth-http** command.

show auth-http

Syntax Description

This command has no arguments or keywords.

Downloaded from www.Manualslib.com manuals search engine

Example

This command and response shows that the WLSE's local authentication is being used for the CLI:

```
show auth-http
local
```

show backupconfig

The **show backupconfig** command displays the current backup and restore configuration.

```
show backupconfig
```

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

To display the current backup and restore configuration, use the **show backupconfig** command. If the backup configuration has not been set, the host and username fields display NONE.

Example

The following command displays the current backup and restore configuration:

```
show backupconfig
Hostname: 209.165.201.0
Username: user1
```

Related Commands

backup

backupconfig

listbackup

restore

Downloaded from www.Manualslib.com manuals search engine

show bootlog

To display the messages logged during the last system boot, use the **show bootlog** command.

show bootlog [page]

Syntax Description

page	Displays command output one screen at a time. Press the **return** key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.

Example

This command displays the messages logged during the last system boot:

```
show bootlog page
Linux/UID32 version 2.2.16-13bipsec.uid32 (gcc version egcs1
Console: colour VGA+ 80x25
Calibrating delay loop... 1133.77 BogoMIPS
start low memory: 0xc0001000 i386_endbase: 0xc009f000
addresses range:: 0xc0f00000  0xc1000000
start memory: c04f8000 end_memory: d0000000
Memory: 257688k/262144k available (988k kernel code, 416k reserved,
2992k data,)
Dentry hash table entries: 262144 (order 9, 2048k)
Buffer cache hash table entries: 262144 (order 8, 1024k)
Page cache hash table entries: 65536 (order 6, 256k)
vmdump: setting dump_execute() as dump_function_ptr ...
VFS: Diskquotas version dquot_6.4.0 initialized
CPU: Intel Pentium III (Coppermine) stepping 06
Checking 386/387 coupling... OK, FPU using exception 16 error
reporting.
Checking 'hlt' instruction... OK.
POSIX conformance testing by UNIFIX
mtrr: v1.35a (19990819) Richard Gooch (rgooch@atnf.csiro.au)
PCI: PCI BIOS revision 2.10 entry at 0xfda95
PCI: Using configuration type 1
-----------more-----------
```


Downloaded from www.Manualslib.com manuals search engine

Related Commands

reload

clock

show cdp neighbor

To display the WLSE's nearest neighbor on the network, use the **show cdp neighbor** command.

show cdp neighbor

Syntax Description

This command has no arguments or keywords.

Example

This command shows the nearest neighbor on the network.

```
show cdp neighbor
cdp neighbor device: Switch
        device type: cisco WS-C2924-XL
        port: FastEthernet0/12
        address: 209.165.201.0
```

show cdp run

To display the Cisco Discovery Protocol (CDP) configuration, use the **show cdp-run** command.

show cdp run

Syntax Description

This command has no arguments or keywords.

Downloaded from www.Manualslib.com manuals search engine

Example

This command displays the CDP configuration:

```
show cdp run
CDP protocol is enabled ...
        broadcasting interval is every 60 seconds.
        time-to-live of cdp packets is 180 seconds.

        CDP is enabled on port eth0.
```

show collectorlog

To display the Wireless LAN Solution Engine's collector log, use the show collectorlog command.

show collectorlog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's collector log, one page at a time:

```
show collectorlog page
/var/adm/CSCOets/log/collector.log
2001/12/20 13:43:18 main HSECollector MESSAGE CollectorMain: Waiting
for databas
e to be ready
2001/12/20 13:43:21 main HSECollector MESSAGE CollectorMain: Database
is ready
SNMPThrPool: Instantiated ex.lib.snmp.lib.timer.DynamicThreadPool,  mi
```


Downloaded from www.Manualslib.com manuals search engine

```
n=15, max=48, maxIdleSecs=0
2001/12/20 13:43:29 main HSECollector MESSAGE ServletServiceModule:
Moxie Servle
t Engine is ready to receive requests
2001/12/20 13:43:30 PeriodicSchedulerRun:FaultCleanup HSECollector
MESSAGE Colle
ctorDBUtils: DB.TableCleanupCommand=[VACUUM ]
2001/12/20 13:43:30 PeriodicSchedulerRun:FaultCleanup HSECollector
MESSAGE Colle
ctorDBUtils: DB.TableUpdateStatsCommand=[VACUUM ANALYZE ]
2001/12/21 10:39:52 Moxie Servlet Engine:Pooled Thread:1 HSECollector
MESSAGE Se
rvletContextAdaptor: Collector: init
```

show config

To display the system configuration, use the **show config** command.

show config

Syntax Description

This command has no arguments or keywords.

Example

This command displays the system configuration:

```
show config
hostname ex1
interface ethernet0 209.165.201.0 255.255.255.224 default-gateway
209.165.202.128
interface ethernet1 down
interface ethernet2 down
interface ethernet3 down
interface ethernet4 down
interface ethernet5 down
ip domain-name embu-doc
ip name-server 209.165.202.158
username admin epassword ************* privilege 15
```


Downloaded from www.Manualslib.com manuals search engine

show daemonslog

To display the Wireless LAN Solution Engine's daemons log, use the **show daemonslog** command.

show daemonslog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's daemons log, one page at a time:

```
show daemonslog page
/var/adm/CSCOets/log/daemons.log
[dmgrDbg] getenv(PX_DBG)=NULL
[dmgrDbg] getenv(PX_MY_DEBUG)=NULL
[dmgrDbg] getenv(PX_MY_TRACE)=NULL
[dmgrDbg] getenv(PX_DBG_LEVEL)=NULL
[dmgrDbg][Thu Dec 20 13:42:53 2001]##### INFO ##### re-evaluate
DbgLevel=0x0
        ++>>it(1) = 8077978 <HSECollector>
        ++>>it(1) = 8077898 <HSEANIServer>
        ++>>it(1) = 8077428 <PostgreSQL>
        ++>>it(1) = 8077228 <WebServer>
        ++>>it(1) = 8077328 <Tomcat>
        ++>>it(1) = 80770d8 <ExcepReporter>
        ++>>it(1) = 8076fc8 <CDPbrdcast>
        ++>>it(1) = 8076e58 <PerfMon>
#!/bin/sh -v
#!/bin/sh -v

if [ "$NMSROOT" = "" ]; then
```


Downloaded from www.Manualslib.com manuals search engine

```
        NMSROOT=/opt/CSCOets
        export NMSROOT
fi

cd $NMSROOT
--More--
```

show dmgtdlog

To display the Wireless LAN Solution Engine's daemon manager log, use the **show dmgtdlog** command.

show dmgtdlog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's daemon manager log, one page at a time:

```
show dmgtdlog page
/var/adm/CSCOets/log/dmgtd.log
Dec 20 13:42:56 ex dmgt[712]: #3001:TYPE=INFO:Using port: tcp/42340.
Dec 20 13:42:56 ex dmgt[714]: #3007:TYPE=INFO:Started application(HSEC
ollector) "/bin/nice -n 19 /opt/CSCOets/bin/collector" pid=715.
Dec 20 13:42:56 ex dmgt[714]: #3007:TYPE=INFO:Started application(HSEA
--More--
```


Downloaded from www.Manualslib.com manuals search engine

show webaccesslog

To display the Wireless LAN Solution Engine's Web access log, use the **show webaccesslog** command.

show webaccesslog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's Web access log, one page at a time:

```
show webaccesslog page
/var/adm/CSCOets/log/access_log
209.165.200.224 - - [21/Dec/2001:10:38:54 +0000] "GET / HTTP/1.0" 302
276 "-" "Moz
illa/4.76 [en]C-CCK-MCD   (Windows NT 5.0; U)"
209.165.200.224 - - [21/Dec/2001:10:38:54 +0000] "GET
/perl/login-form.cgi HTTP/1.
0" 200 2268 "-" "Mozilla/4.76 [en]C-CCK-MCD   (Windows NT 5.0; U)"
209.165.200.224 - - [21/Dec/2001:10:38:55 +0000] "GET /icons/hse.gif
HTTP/1.0" 200
 5554 "http://209.165.201.0:1741/perl/login-form.cgi" "Mozilla/4.76
[en]C-CCK-MC
D   (Windows NT 5.0; U)"
209.165.200.224 - - [21/Dec/2001:10:38:55 +0000] "GET
/icons/left_top.gif HTTP/1.0
" 200 324 "http://209.165.201.0:1741/perl/login-form.cgi"
"Mozilla/4.76 [en]C-CC
K-MCD   (Windows NT 5.0; U)"
--More--
```


Downloaded from www.Manualslib.com manuals search engine

show weberrorlog

To display the Wireless LAN Solution Engine's Web error log, use the **show weberrorlog** command.

show weberrorlog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's Web error log, one page at a time:

```
show weberrorlog page
/var/adm/CSCOets/log/error_log
[Thu Dec 20 13:43:00 2001] [error] (22)Invalid argument: <Perl>:
Invalid command
 'secret', perhaps mis-spelled or defined by a module not included in
the server
 configuration
[Thu Dec 20 13:43:00 2001] [error] (22)Invalid argument: <Perl>:
Invalid command
 'line', perhaps mis-spelled or defined by a module not included in
the server c
onfiguration
[Thu Dec 20 13:43:00 2001] [error] (22)Invalid argument: <Perl>:
```


Downloaded from www.Manualslib.com manuals search engine

show webssslaccesslog

To display the Wireless LAN Solution Engine's Web SSL log, use the **show webssslaccesslog** command.

show webssslaccesslog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's Web SSL log, one page at a time:

```
show webssslaccesslog page
```

show import

To display an imported host file, use the **show import** command.

show import *hosts*

Syntax Description

hosts	Name of server that host files were imported from.

Downloaded from www.Manualslib.com manuals search engine

Example

This command displays the imported host file

```
show import ftpserver_1
```

show install logs

To display the software updates and images available on the configured repository, use the **show install logs** command.

show install logs [short | long] [page]

Syntax Description

short	Displays only the names of software updates and images on the configured repository
long	Displays the names and descriptions of software updates and images on the configured repository.
page	Displays command output one screen at a time.

Example

The following command displays the software updates and images available on the configured browser, one screen at a time:

```
show install updates page
2
NAME=EX-2.0a
```

show ipchains

To display the IP chains for the selected interface, use the **show ipchains** command.

show ipchains *eth<0-5>*

Downloaded from www.Manualslib.com manuals search engine

Syntax Description

eth<0-5>	Name of the interface port to be configured. Acceptable values are eth0-5.

Example

The following command displays the IP chains for the ethernet 0 interface:

```
show ipchains eth0
Chain ineth0 (1 references):
target     prot opt     source               destination
ports
ACCEPT     tcp  -y--l-  anywhere             ex.help     any ->   telt
ACCEPT     tcp  ------  anywhere             ex.help     any ->   telt
ACCEPT     tcp  ------  anywhere             ex.help     any ->   3345
ACCEPT     tcp  -y--l-  anywhere             ex.help     any ->   ssh
```

show hosts

To display your Wireless LAN Solution Engine's host file, use the **show hosts** command.

show hosts [page]

Syntax Description

page	Displays command output one screen at a time.

Example

The following command displays your Wireless LAN Solution Engine's host file one page at a time:

```
show hosts page
```


Downloaded from www.Manualslib.com manuals search engine

show maillog

To display the Wireless LAN Solution Engine's mail log, use the **show maillog** command.

show maillog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's collector log, one page at a time:

```
show maillog page
/var/log/maillog
Dec 21 04:02:06 ex sendmail[11643]: EAA11643: from=root, size=307, cla
ss=0, pri=30307, nrcpts=1, msgid=<200112210402.EAA11643@ex.help>, rela
y=root@localhost
Dec 21 04:02:06 ex sendmail[11660]: EAA11643: SYSERR(root): Cannot exe
c /usr/bin/procmail: No such file or directory
Dec 21 04:02:06 ex sendmail[11643]: EAA11643: to=root, ctladdr=root (0
/0), delay=00:00:06, xdelay=00:00:00, mailer=local, stat=Operating
system error
```

show proc

To display the Wireless LAN Solution Engine's active process statistics, use the **show proc** command.

show proc [page]

Downloaded from www.Manualslib.com manuals search engine

Syntax Description

page	Displays command output one screen at a time.

Example

The following command displays the Wireless LAN Solution Engine's active process statistics one page at a time:

```
show proc page
PID     ELAPSED    SZ                  STARTED TTY  COMMAND
    1    22:29:10   277 Thu Dec 20 13:42:29 2001 ?    init
    2    22:29:10     0 Thu Dec 20 13:42:29 2001 ?    kflushd
    3    22:29:10     0 Thu Dec 20 13:42:29 2001 ?    kupdate
    4    22:29:10     0 Thu Dec 20 13:42:29 2001 ?    kpiod
    5    22:29:10     0 Thu Dec 20 13:42:29 2001 ?    kswapd
    6    22:29:03     0 Thu Dec 20 13:42:36 2001 ?    kreiserfsd
   85    22:29:00     0 Thu Dec 20 13:42:39 2001 ?    kreiserfsd
   86    22:29:00     0 Thu Dec 20 13:42:39 2001 ?    kreiserfsd
   87    22:28:59     0 Thu Dec 20 13:42:40 2001 ?    kreiserfsd
   88    22:28:59     0 Thu Dec 20 13:42:40 2001 ?    kreiserfsd
   89    22:28:59     0 Thu Dec 20 13:42:40 2001 ?    kreiserfsd
  208    22:28:57   290 Thu Dec 20 13:42:42 2001 ?    watchdog
  322    22:28:51   342 Thu Dec 20 13:42:48 2001 ?    idled
  510    22:28:51   290 Thu Dec 20 13:42:48 2001 ?    syslogd
  519    22:28:50   361 Thu Dec 20 13:42:49 2001 ?    klogd
  637    22:28:48   327 Thu Dec 20 13:42:51 2001 ?    crond
  651    22:28:48   286 Thu Dec 20 13:42:51 2001 ?    inetd
17076       18:23   364 Fri Dec 21 11:53:16 2001 ?     \_ in.telnetd
17077       18:23   575 Fri Dec 21 11:53:16 2001 0     |   \_ login
-----------more-----------
```

show repository

To display the status or the access log of a configured repository, use the **show repository** command.

show repository {status | access-log} [page]

Syntax Description

status	Displays the status of the local repository
access-log	Displays the access-log of the local repository

Downloaded from www.Manualslib.com manuals search engine

page Displays command output one screen at a time.

Example

This command displays the status of the configured repository:

```
show repository status
Repository Source: 171.69.212.146:9851
repository is running.
```

show route

To display the routes currently configured, use the show route command.

show route

Syntax Description

This command has no arguments or keywords.

Example

This command displays the currently configured routes

```
show route
Destination     Gateway Genmask         Flags Metric Ref    Use Iface
209.165.200.224 0.0.0.0 255.255.255.224 UH    0      0        0 eth0
209.165.200.225 0.0.0.0 255.255.255.224 U     0      0        0 eth0
209.165.200.254 0.0.0.0 255.255.255.224 U     0      0        0 lo
209.165.202.128 0.0.0.0 255.255.255.224 UG    0      0        0 eth0
```

show securitylog

To display the Wireless LAN Solution Engine's security log information, use the **show securitylog** command.

show securitylog [page] | include *matchstring1 [matchstring2]*

Downloaded from www.Manualslib.com manuals search engine

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's security log, one page at a time:

```
show securitylog page
/var/log/secure
Dec 20 13:45:23 ex in.tftpd[1381]: connect from 209.165.200.224
Dec 20 13:45:27 ex in.tftpd[1383]: connect from 209.165.200.224
Dec 20 13:45:31 ex in.tftpd[1385]: connect from 209.165.200.224
Dec 20 13:45:35 ex in.tftpd[1387]: connect from 209.165.200.224
Dec 20 13:45:39 ex in.tftpd[1389]: connect from 209.165.200.224
Dec 20 13:45:44 ex in.tftpd[1391]: connect from 209.165.200.224
Dec 20 13:45:48 ex in.tftpd[1393]: connect from 209.165.200.224
Dec 20 13:45:52 ex in.tftpd[1395]: connect from 209.165.200.224
Dec 20 13:45:56 ex in.tftpd[1397]: connect from 209.165.200.224
Dec 20 13:46:00 ex in.tftpd[1399]: connect from 209.165.200.224
Dec 20 13:46:04 ex in.tftpd[1412]: connect from 209.165.200.224
Dec 20 13:46:27 ex in.tftpd[1424]: connect from 209.165.200.224
Dec 20 13:46:31 ex in.tftpd[1426]: connect from 209.165.200.224
Dec 20 13:46:35 ex in.tftpd[1428]: connect from 209.165.200.224
Dec 20 13:46:39 ex in.tftpd[1430]: connect from 209.165.200.224
Dec 20 13:46:43 ex in.tftpd[1432]: connect from 209.165.200.224
Dec 20 13:46:47 ex in.tftpd[1434]: connect from 209.165.200.224
--More--
```


Downloaded from www.Manualslib.com manuals search engine

show snmp-server

To display the Wireless LAN Solution Engine's SNMP configuration, use the **show snmp-server** command.

show snmp-server

Syntax Description

This command has no arguments or keywords.

Example

The following command displays the Wireless LAN Solution Engine's SNMP configuration:

```
show snmp-server
RW community string: private
        RO community string: public

        sysLocation: your site information
        sysContact: your contact information

        trap-forwarding is disabled
```

show ssh-version

To display the type of SSH enabled, use the ssh-version command.

show ssh-version

Syntax Description

This command has no arguments or keywords.

Example

This command displays the type of SSH that is enabled:

```
show ssh-version
SSH1, SSH2
```


Downloaded from www.Manualslib.com manuals search engine

show syslog

To display syslog information, use the **show syslog** command.

show syslog [page] [include *matchstring1* **[***matchstring2***]]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Usage Guidelines

Use this command to display syslog information.

To filter the command output to include only the records that contain the specified string(s) of characters, use the **include** option with one or two character strings to search for. If you include two strings, the command outputs only those records that contain both character strings.

Example

This command displays syslog information:

```
show syslog
Jun 20 16:04:23 ex syslogd 1.3-3: restart.
Jun 20 16:04:23 ex syslog: syslogd startup succeeded
Jun 20 16:04:23 ex kernel: klogd 1.3-3, log source = /proc/kmsg start.
Jun 20 16:04:23 ex kernel: Inspecting /boot/System.map-2.2.16-13bipse2
Jun 20 16:04:23 ex syslog: klogd startup succeeded
-----------more-----------
```

Related Command

interface

Downloaded from www.Manualslib.com manuals search engine

show tech

To display information necessary for Cisco's Technical Assistance Center to assist you, use the **show tech** command.

show tech [page]

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.

Example

This command displays system information necessary for Cisco's Technical Assistance Center to assist you.

```
show tech page
/bin/cat: /var/log/secure: Permission denied
Copyright (c) 1999-2000 by Cisco Systems, Inc.
Build Version (166) Mon Jun 11 16:56:23 PDT 2001
Linux/UID32 version 2.2.16-13bipsec.uid32 (gcc version egcs1
Uptime: 0 days 18 hours 35 mins

2 Ethernet interfaces
hostname ex
interface ethernet0 209.165.200.224 255.255.255.224 default-gateway
209.165.202.128
ip name-server 209.165.201.0
username admin epassword ************* privilege 15
eth0      Link encap:Ethernet  HWaddr 00:02:B3:35:FD:CC
          inet addr:209.165.200.224 Bcast:209.165.201.31
Mask:255.255.255.224
-----------more-----------
```

show telnetenable

To display the Wireless LAN Solution Engine's Telnet status, use the **show telnetenable** command.

show telnetenable

Downloaded from www.Manualslib.com manuals search engine

Syntax Description

This command has no arguments or keywords.

Example

The following command shows if Telnet is enabled or disabled:

```
show telnetenable
telnet enable for: ALL
```

show tomcatlog

To display the Wireless LAN Solution Engine's Tomcat log, use the **show tomcatlog** command.

show tomcatlog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's tomcat log, one page at a time:

```
show tomcatlog page
/var/adm/CSCOets/log/tomcat.log
2001-12-20 01:43:06 - ContextManager: Adding context Ctx( /examples )
2001-12-20 01:43:06 - ContextManager: Adding context Ctx( /admin )
Starting tomcat. Check logs/tomcat.log for error messages
2001-12-20 01:43:06 - ContextManager: Adding context Ctx(  )
getUIProperties(): unhandled error could be a bad ui.properties
```


Downloaded from www.Manualslib.com manuals search engine

```
java.lang.NullPointerException
        at java.io.Reader.<init>(Reader.java:68)
        at java.io.InputStreamReader.<init>(InputStreamReader.java:96)
--More--
```

shutdown

To shut down the system in preparation for powering it off, use the **shutdown** command.

shutdown

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to shut down the WLSE in preparation for powering it off. All processes running on the WLSE will stop, and it will not respond until you power it off and back on.

You are prompted to verify the shutdown. Enter **yes** to continue, or **no** to cancel the shutdown.

Caution Never power the system off without running the **shutdown** command first. Doing so can destroy data and prevent the system from booting.

Example

This command shuts down the system:

```
shutdown
```

Related Commands

reload

Downloaded from www.Manualslib.com manuals search engine

snmp-server

To configure a simple network management protocol (SNMP) agent, use the **snmp-server** command.

snmp-server {community *community-name* **[RO|RW] | location** *sysLocation-info* **| contact** *sysContact-info***}**

no snmp-server {community *community-name* **| location | contact}**

Syntax Description

community	sets the community strings that permit access to the SNMP.
community-name	the community name string.
RO	read only.
RW	read / write.
location	sets the system location string.
sysLocation-info	the location string.
contact	sets the contact string.
sysContact-info	the contact string.

Example

This command sets an SNMP contact string:

```
snmp-server contact Dial System Operator at Beeper # 27345
```

ssh

To use SSH to connect to an external host, use the ssh command.

ssh [*options***]** *host* **[***command***]**

Downloaded from www.Manualslib.com manuals search engine

Syntax Description

options	Standard SSH options. For a list of these options, enter the **ssh** command without any arguments.
host	Name or IP address of host to which to connect.
command	Command for the external host to execute.

Example

Enter the following command to connect to an external host using SSH:

```
ssh 209.165.200.224
```

ssh-version

Use the ssh-version command to enable Secure Shell (SSH) 1, SSH 2, or both SSH 1 and SSH 2.

ssh-version {ssh1 | ssh2 | both}

Syntax Description

ssh1	Enables SSH 1
ssh2	Enables SSH 2
both	Enables both SSH 1 and SSH2

Example

This command enables ssh1:

```
ssh-version ssh1
```

telnet

To Telnet to an external host, use the telnet command.

telnet {*hostname* | *ip-address***} [***portnumber***]**

Downloaded from www.Manualslib.com manuals search engine

Syntax Description

hostname	Hostname of the external device.
ip-address	IP address of the external device.
portnumber	portnumber of the external device.

Example

Enter the following command to telnet to port 9851 of a system with the IP address 209.165.200.224:

```
telnet 209.165.200.224 9851
```

telnetenable

To configure Telnet access, use the **telnetenable** command.

telnetenable {enable [*ip-addresses* **|** *domains***] | disable | status}**

Syntax Description

enable	Enables Telnet access to the system.
disable	Disables Telnet access to the system.
status	Displays current access status.
ip-addresses	IP addresses of systems allowed Telnet access. If this argument is used, no other machines will be allowed access. Multiple IP address are allowed.
domains	Domains of systems allowed Telnet access. If this argument is used, machines with domains other than the specified domain will be denied Telnet access. Multiple domains are allowed.

Default

The default is **disable**.

Downloaded from www.Manualslib.com manuals search engine

Usage Guidelines

To enable Telnet access to the system for *all* IP source addresses, use the **telnetenable enable** command alone. To enable *specific* IP addresses, use the **telnetenable enable** command followed by the IP addresses.

Example

This command enables Telnet for all IP source addresses:

```
telnetenable enable
```

username

To create a new user account or change an account's properties, use the **username** command. Use the **no** form of the command to remove a user account.

username *name* **password** *password* **[privilege {0 | 15}]**

no username *name*

Syntax Description

name	Name of the user account to create or remove.
password	Specifies a password for the account.
password	The password for the account.
privilege	(Optional) Specifies the account privilege level.
0	Gives the account level 0 privileges. This is the default.
15	Gives the account level 15 privileges.

Downloaded from www.Manualslib.com manuals search engine

Usage Guidelines

Use the **username** command to change the properties of a user account. To assign a user CLI privilege level 15, use the **username** command. You cannot assign CLI privilege level 15 through the Web interface. Use the **no** form of the command to remove a user account. The default privilege level is 0 if you do not provide the privilege option.

For more information about managing user accounts and privilege levels, refer to Administering Users, page 6-75.

Example

This command creates a user account named user1 with password password1 and privilege level 15:

```
username user1 password password1 privilege 15
```

This command removes the user account:

```
no username user1
```

Maintenance Image Commands

This section describes the commands that are available when the system is booted from the maintenance image. For more information about the maintenance image, refer to the *Installation and Configuration Guide for the Cisco 1105 Wireless LAN Solution Engine*.

erase config

This command is identical to the level 15 **erase config** command. For a description, see the "erase config" section on page B-23.

Downloaded from www.Manualslib.com manuals search engine

fsck

To check and repair the filesystem, use the fsck command.

fsck

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use the **fsck** command to check and repair the filesystem. The command might prompt you for confirmation before making certain repairs.

Example

The following command checks and repairs the filesystem:

```
fsck
```

reload

This command is identical to the level 15 **reload** command. For a description, see "reload" section on page B-39.

Downloaded from www.Manualslib.com manuals search engine

A

AAA — Authentication, Authorization, and Accounting. The WLSE monitors LEAP, EAP-MD5 and RADIUS AAA services provided by AAA servers running CiscoSecure ACS Server software.

See also EAP-MD5 server, LEAP server, and RADIUS.

access point — Access points are wireless LAN transceivers that serve as the center point of a standalone wireless network or as the connection point between wireless and wired networks. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

ANI — Asynchronous Network Interface. A mediation layer between the network devices and client applications. ANI provides discovery, inventory, and topological computations of networks and their devices

B

BDPU — Bridge Protocol Data Unit. *See* STP.

BOOTP — Bootstrap Protocol. The protocol used by a network node to determine the IP address of its Ethernet interfaces to affect network booting.

bridge — *See* wireless bridge.

Downloaded from www.Manualslib.com manuals search engine

C

CDP Cisco Discovery Protocol. Media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. Using Cisco Discovery Protocol, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. Runs on all media that support SNAP, including LANs, Frame Relay, and ATM media.

CDP distance The CDP distance determines the depth of the discovery and applies to all seed devices. If CDP distance is 1, only the immediate neighbors of the seed device are discovered. If CDP distance is 2, devices A and B that are directly connected to the seed devices are discovered and the immediate neighbors of A and B are also discovered.

CLI The command line interface for administering the WLSE. You use the CLI through a console attached to the WLSE's console port or by opening a Telnet connection to the WLSE. CLI commands are described in the *User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*—from the online help, click **PDF**.

community strings Text strings that act as passwords to authenticate communication with devices that contain an SNMP agent.

CoS Class or Service. An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages.

CSR Certificate Signed Request. Request sent to a certificate authority for using HTTPS.

D

DHCP Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

Downloaded from www.Manualslib.com manuals search engine

DNS Domain Name System. An Internet service that translates domain names into IP addresses. Domain names are a clear way of representing an Internet address. The Internet, however, is actually based on IP addresses. For example, the URL http //www.website.com might actually point to the IP address http //123.456.789.0. Because maintaining a central list of domain name/IP address correspondences would be impractical, the lists of domain names and IP addresses are distributed throughout servers on the Internet in the Domain Name System. If one DNS server cannot translate a particular domain name, it contacts another one, and so on, until the correct IP address is returned.

DTIM Deliver Traffic Indication Message. Used by access points to tell power-save client devices that a packet is waiting for them.

DSCP Differentiated Services Code Point is a model in which traffic is treated by intermediate systems with relative priorities based on the type of services.

E

EAP-MD5 server Servers running extensible authentication protocol to provide dynamic, session-specific wireless encryption keys, central user administration. and authentication between clients and access points. EAP-MD5 uses MD5 hashing on client and challenge passwords. The WLSE monitors EAP-MD5 servers.

See also AAA.

exception A group of related faults.

H

HTTP Hypertext Transfer Protocol. The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.

HTTPS Secure HTTP with SSL (secure socket layer). *See also* SSL.

Downloaded from www.Manualslib.com manuals search engine

I

ICMP Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.

L

LEAP server Light EAP server, which combines centralized two-way authentication with dynamically generated wireless equivalent privacy keys or WEP keys.

See also AAA and WEP keys.

M

MIC Media Interface Connector. FDDI de facto standard connector.

MOK A type of modulation used before the IEEE finished high-speed 802.11 standard and may still be used in older wireless networks.

N

nslookup The NSLookup tool is used to look up device or host information via the name server. You must enter a device name, not an IP address, to use this function. You must have a DNS server in order to look up network servers.

NTP Network Time Protocol. Protocol built on top of TCP that ensures accurate local timekeeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

Downloaded from www.Manualslib.com manuals search engine

P

ping A common method for troubleshooting the accessibility of devices.

A ping tests an ICMP echo message and its reply. Because ping is the simplest test for a device, it is the first to be used. If ping fails, try using traceroute.

Run ping to view the packets transmitted, packets received, percentage of packet loss, and round-trip time in milliseconds.

PSPF Publicly Secure Packet Forwarding. A feature that prevents client devices associated to a bridge or access point from inadvertently sharing files with other client devices on the wireless network.

Q

QoS Quality of Service. Measure of performance for transmission systems that reflects their transmission quality and service availability.

R

RADIUS Remote Authentication Dial-In User Service. Database for authenticating connections and for tracking connection time. The WLSE monitors RADIUS servers. The WLSE also provides a RADIUS module for authenticating users.

See also AAA.

repository The Repository provides software update services to the Solution Engine. You can download software from the Repository and install it on the Solution Engine, and you can browse the available software versions on the Repository.

Downloaded from www.Manualslib.com manuals search engine

S

seed A CDP-enabled device used as a starting point for discovery. For example, by adding a seed device (or set of seed devices), the neighbors of the seed device are discovered using CDP.

SMTP Simple Mail Transfer Protocol. Internet protocol providing e-mail services.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SSH Secure Shell. Provides a secure Telnet connection, encrypting all traffic, including passwords

SSID Service Set ID. It is a unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity. The SSID can be any alphanumeric entry up to 32 characters long.

SSL Secure Socket Layer. Proves a secure connection between the WLSE and Web clients.

STP Spanning-Tree Protocol. Bridge protocol that uses the spanning-tree algorithm, enabling a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange BPDU messages with other bridges to detect loops, and then remove the loops by shutting down selected bridge interfaces. Refers to both the IEEE 802.1 Spanning-Tree Protocol standard and the earlier Digital Equipment Corporation Spanning-Tree Protocol upon which it is based. The IEEE version supports bridge domains and allows the bridge to construct a loop-free topology across an extended LAN. The IEEE version generally is preferred over the Digital version.

Downloaded from www.Manualslib.com manuals search engine

T

TACACS+ Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.

TCP Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

TFTP Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).

threshold A range within which you expect your network to perform. If a threshold is exceeded or goes below the expected bounds, you examine the areas for potential problems. You can create thresholds for a specific device.

TKIP Temporal Key Integrity Protocol, also known as key hashing, is used as part of server-based EAP authentication.

traceroute This is a diagnostic tool that helps you understand why ping fails or why applications time out. Using it, can view each hop (or gateway) on the route to your device and how long each took.

U

UTC Coordinated Universal Time. Time zone at zero degrees longitude. Formerly called Greenwich Mean Time (GMT) and Zulu time.

Downloaded from www.Manualslib.com manuals search engine

V

VLAN Virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLAN ID Virtual Local Area Network identification used by the standard 802.1Q. Being on 12 bits, it allows the identification of 4096 VLANs.

W

WEP keys Wired equivalent privacy (WEP) keys are the IEEE 802.11b standard that offers a mechanism for securing wireless LAN data streams. The goals of WEP include access control to prevent unauthorized users who lack a correct WEP key from gaining access to the network, and privacy to protect wireless LAN data streams by encrypting them and allowing de-encryption only by users with the correct WEP keys.

wireless bridge Designed to connect two or more networks (typically located in different buildings). Bridges connect hard-to-wire sites, noncontiguous floors, satellite offices, school or corporate campus settings, temporary networks, and warehouses. For functional flexibility, the wireless bridge may also be configured as an access point.

Downloaded from www.Manualslib.com manuals search engine

Numerics

11a radio, configuring 3-73
- advanced 3-81
- data encryption 3-89
- filters 3-75
- hardware 3-76
- identification 3-73
- searched channels 3-88

11b radio, configuring 3-56
- advanced 3-66
- filters 3-59
- hardware 3-60
- identification 3-56
- searched channels 3-71

A

AAA
- definition GL-1
- server, adding 6-33
- server, setting up 6-16

access point
- AP and bridge connected to router report, displaying 5-48
- AP and bridge connected to switch report, displaying 5-46
- configuring 3-1
- current client association report, displaying 5-29
- definition GL-1
- detailed report, displaying 5-26
- Ethernet transmission statistics, displaying 5-58
- Ethertype protocol filters report, displaying 5-32
- faults, displaying 2-2
- fault thresholds, setting 2-7
- firmware, updating 4-1
- group performance report
  - Ethernet utilization, displaying 5-53
  - RF utilization, displaying 5-51
- group policy report, displaying 5-21
- group report, displaying 5-12
- group security report, displaying 5-14
- group SSID report, displaying 5-16
- group VLAN report, displaying 5-18
- HTTP username and password, specifying 6-9
- IP port filters report, displaying 5-35
- IP protocol filters report, displaying 5-33
- limitation on number of 6-4

Downloaded from www.Manualslib.com manuals search engine

performance graph, displaying 5-60
performance table, displaying 5-61
per VLAN client (group) report, displaying 5-20
per VLAN client (individual) report, displaying 5-43
policy report, displaying 5-36
policy settings 2-7
QBSS QoS report, displaying 5-38
RF transmission statistics, displaying 5-56
setting up 6-12
SSID report, displaying 5-40
summary report, displaying 5-24
system-defined groups for 6-37
template, creating 3-132
top n busiest clients, displaying 5-62
top n client error rate report, displaying 5-64
top n number of associations report, displaying 5-54
top n percentage errors report, displaying 5-55
VLAN report, displaying 5-42
accounting, configuring 3-119
address filters, configuring 3-12
advanced associations, configuring 3-42
advanced settings, Ethernet port 3-53
aggregation interval, setting 6-73
Aggregation Truncation Interval, setting 6-73
ANI
definition GL-1
log, displaying B-48
AP Ethertype protocol filters report, displaying 5-32
AP IP port filters report, displaying 5-35
AP IP protocol filters report, displaying 5-33
AP policy report, displaying 5-36
AP QBSS QoS report, displaying 5-38
AP SSID report, displaying 5-40
AP summary report, displaying 5-24
AP VLAN report, displaying 5-42
associations, setting up
address filters 3-12
advanced 3-42
DSCP to CoS 3-48
Ethertype filters 3-14
IP port filters 3-23
IP protocol filters 3-18
policy groups 3-28
port assignments 3-47
quality of service 3-36
service sets 3-38
VLANs 3-31
audience for this document xiii
auth command B-17
authentication
enabling B-17
for CLI access, displaying B-49
for HTTP access, displaying B-49
modules supported 6-56
overview 6-56
setting up 6-57

Downloaded from www.Manualslib.com manuals search engine

troubleshooting 8-14
auto-managed configuration 3-154
assigning 3-156
options for email 3-157
Auto-Manage devices 6-18
automatic configurations, creating 3-151

B

backing up and restoring WLSE configuration
backup location, configuring 6-61, B-19
backup location, Windows server 6-62
backup procedure 6-63, B-18
backups, listing B-33
configuring backup B-19, B-50
restore procedure 6-64
restoring configuration B-45
backup command B-18
backupconfig command B-19
booting, WLSE 6-47, B-39, B-51
bridge
AP and bridge connected to router report, displaying 5-48
AP and bridge connected to switch report, displaying 5-46
configuring 3-1
current client association report, displaying 5-29
definition GL-1
detailed report, displaying 5-26
Ethernet transmission statistics 5-58
firmware, updating 4-1
group performance report
Ethernet utilization, displaying 5-53
RF utilization, displaying 5-51
group policy report, displaying 5-21
group report, displaying 5-12
group security report, displaying 5-14
group SSID report, displaying 5-16
group VLAN report, displaying 5-18
limitation on number of 6-4
performance graph, displaying 5-60
per VLAN client (group) report, displaying 5-20
per VLAN client (individual) report, displaying 5-43
RF transmission statistics, displaying 5-56
setting up 6-12
template, creating 3-132
top n number associations report, displaying 5-54
top n percentage errors report, displaying 5-55
browser
date and time display 1-5

C

cautions
erase config command B-23

Downloaded from www.Manualslib.com manuals search engine

losing data by clicking between subtabs 3-138, 4-10
reload command B-39
shutdown command, failure to run B-70
significance of xiv
CDP (Cisco Discovery Protocol)
configuring B-20, B-52
definition GL-2
neighbors, displaying B-52
template 3-112
use in discovery 6-11
cdp command B-20
CDP distance
definition of GL-2
setting 6-20
CD-ROM, obtaining Cisco documentation on xvi
character set, allowable A-1
Cisco.com
importing firmware from 4-7
obtaining technical assistance through xvii
CiscoSecure ACS Server, configuring 6-16
CiscoWorks2000
exporting devices to 6-31
importing devices from 6-30
linking to CiscoWorks2000 server 6-81
CLI
access, configuring 6-77
commands B-1
definition GL-2
using B-2
CLI commands
conventions B-2
use of quotes B-2
client
current association report, displaying 5-29
detail report, displaying 5-6
historical association report, displaying 5-9
inventory of associations 6-24
per VLAN (group) report, displaying 5-20
per VLAN (individual) report, displaying 5-44
statistics report, displaying 5-8
top n busiest report, displaying 5-62
top n error rate, displaying 5-64
clock command B-21
collector log, displaying B-53
command reference B-1
CLI conventions B-2
command history feature B-3
command privileges B-2
command summary (table) B-4
help for B-3
maintenance image commands B-75
erase config B-75
fsck B-76
reload B-76
Privilege Level 0 commands B-10
exit B-10
ping B-10

Downloaded from www.Manualslib.com manuals search engine

show clock B-11
show domain-name B-12
show interfaces B-13
show process B-13
show version B-14
traceroute B-15
Privilege Level 15 commands B-17
auth B-17
backup B-18
backupconfig B-19
cdp B-20
clock B-21
erase config B-23
firewall B-24
gethostbyname B-25
hostname B-25
import B-26
interface B-30
ip domain-name B-31
ip name-server B-32
listbackup B-33
mail B-34
mailcntrl clear B-35
mailcntrl list B-35
mailroute B-36
nslookup B-36
ntp server B-37
reload B-39
restore B-45
route B-46
services B-46
show auth-cli B-49
show auth-http B-49
show backupconfig B-50
show bootlog B-51
show cdp-neighbor B-52
show cdp-run B-52
show config B-54
show import B-59
show route B-64
show ssh-version B-66
show syslog B-67
show tech B-68
shutdown B-70
snmp-server B-71
ssh-version B-72
telnetenable B-73
username B-74
syntax, checking B-2
typographical conventions B-9
community strings
definition GL-2
guidelines 6-9
requirement for 6-7
setting on devices 6-12
specifying 6-7
configuration, WLSE
backing up 6-61, B-18

Downloaded from www.Manualslib.com manuals search engine

displaying B-54
restoring 6-61, B-45
configuration history, viewing device's 5-1
configuring devices
configuration jobs 3-137
devices, setting up for discovery 6-12
firmware, updating 4-1
templates, using 3-1
troubleshooting 8-3
connectivity, testing 6-72
console/Telnet services, configuring 3-107
conventions
CLI B-2
in command descriptions B-9
CoS (class of service), configuring from DSCP 3-48
credentials, devices 6-6
current reports, displaying 5-11
AP and bridge connected to router report 5-48
AP and bridge connected to switch report 5-46
AP Ethertype protocol filters report 5-32
AP IP port filters report 5-35
AP IP protocol filters report 5-33
AP policy report 5-36
AP QBSS Qos report 5-38
AP SSID report 5-40
AP summary 5-24
AP VLAN report 5-42
current client association 5-29
detailed 5-26
EAP authentication 5-30
group 5-12
group policy report 5-21
group security 5-14
group SSID 5-16
group VLAN 5-18
per VLAN (group) client report 5-20
per VLAN client (individual) report 5-43
router summary 5-47
server summary report 5-49
switch summary 5-45
custom values, configuring 3-130

D

daemon log, displaying 6-46
daemon manager log, displaying 6-46, B-56
database
backing up 6-61, B-18, B-19, B-50
checking database status 7-1
reinitializing B-40
restoring 6-61, B-45, B-50
date and time
displaying B-11
in WLSE displays 1-5
setting client time 6-69
setting system time B-21

Downloaded from www.Manualslib.com manuals search engine

synchronizing to a time server 6-70, B-37
deleting
devices 6-3
groups 6-43
users 6-80, B-74
detailed report, displaying 5-26
device center 5-1
Device Credentials option 6-6
Device History option 6-5
device names
displaying 6-18
translating to IP addresses B-36
devices
configuring
configuration jobs 3-138
setting up for discovery 6-12
templates 3-1
troubleshooting 8-3
connectivity, testing 6-72
credentials, setting 6-6
deleting 6-3
details, viewing 6-3
device name, display of 1-5
exporting to CiscoWorks2000 6-31
fault summary, viewing 5-1
firmware, updating 4-1
grouping 6-37
history viewing 5-1
importing
from CiscoWorks2000 6-30
from file 6-29
limitation on number of wireless devices 6-4
management history 6-5
managing 6-2
newly discovered 6-3
setting up 6-12
unmanaged 6-3
diagnostics, WLSE
processes, viewing 6-68
self-test 6-65
status reports 6-65
discovery
CDP
CDP distance, setting 6-11
configuring B-20
enabling on access points and bridges 6-12
enabling on routers and switches 6-15
device setup for 6-12
enabling 6-20
filters 6-19
history 6-27
immediate 6-22
importing devices 6-28
newly discovered devices 6-3
one-time 6-22
options 6-10
overview 6-11
scheduling 6-20

Downloaded from www.Manualslib.com manuals search engine

seed devices 6-20
troubleshooting 8-13
disk
checking and repairing B-76
usage, viewing B-22
DNS
configuring 3-113
definition GL-3
name servers, specifying 6-71, B-32
reverse lookup 1-5
effect on device name display 6-18
specifying 6-18
documentation
feedback, providing electronically or by mail xvi
obtaining xv
on a CD-ROM xvi
on the World Wide Web xv
ordering xvi
related xiv
domain name
default, defining B-31
displaying B-12
DSCP to CoS, configuring 3-48

E

EAP-MD5 server
adding 6-36
authentication report, displaying 5-30
definition GL-3
setting up 6-16
summary report, displaying 5-49
email
automatic configuration results 3-157
faults 2-23
forwarding B-36
logs and queues B-35, B-62
mail server, specifying 6-71
notification settings 2-23
report 5-66
scheduling 5-68
testing and debugging B-34
troubleshooting 8-10
erase config command B-23, B-75
Ethernet filters, configuring for port 3-50
Ethernet port, configuring 3-49
advanced settings 3-53
filters 3-50
hardware 3-52
identification 3-49
Ethertype filters, configuring 3-14
event handling, configuring 3-124
event notification, configuring 3-129
events, configuring 3-124
handling 3-124
notification 3-129
exception, definition GL-3
exit command B-10

Downloaded from www.Manualslib.com manuals search engine

exporting
devices 6-31
reports 5-66
templates 3-137
express template, using 3-3

F

fault history truncation interval, setting 6-73
faults
displaying 2-1
emailing 2-23
exception, definition of GL-3
faults log (WLSE), displaying 6-46
notification settings 2-20
emailing faults 2-23
syslog 2-22
trap notification 2-21
troubleshooting email 8-2
parameters for fault reporting 6-73
thresholds, specifying 2-7
filters
AP Ethertype protocol report, displaying 5-32
AP IP port report, displaying 5-35
AP IP protocol report, displaying 5-33
Ethernet, configuring 3-50
Ethertype, configuring 3-14
IP port, configuring 3-23
IP protocol, configuring 3-19
firewall command B-24
firmware
history, viewing device's 5-1
updating 4-1
fsck command B-76
FTP, configuring 3-114

G

gateway, specifying B-30
gethostbyname command B-25
getting started with WLSE 1-1
group performance report
Ethernet utilization 5-53
RF utilization 5-51
group report, displaying 5-12
groups
copying 6-41
creating 6-39
deleting 6-39
editing 6-39
overview 6-37
performance report for Ethernet utilization, displaying 5-53
performance report for RF utilization, displaying 5-51
per VLAN client report, displaying 5-20
policy report, displaying 5-21
report, displaying 5-12
security report, displaying 5-14

Downloaded from www.Manualslib.com manuals search engine

SSID report, displaying 5-16
system-defined 6-37
top number of associations report, displaying 5-54
top percentage errors report, displaying 5-55
VLAN report, displaying 5-18
GUI
About button 1-4
buttons 1-4
device name display 1-5
display of sysName in 1-5
Help button 1-4
Logout button 1-4
tabs and subtabs 1-2
time display 1-5
timeout period 1-2

H

hardware configuration, Ethernet port 3-52
help
CLI, displaying B-3
online xv
technical assistance, obtaining xvi
Cisco.com xvii
TAC xvii
host file
displaying B-59, B-61
importing B-26
hostname
changing system hostname B-25
translating to IP addresses B-36
hostname command B-25
hot standby, configuring 3-109
HTTP
definition GL-3
setting on access points 6-12
template 3-116
username and password for access points, specifying 6-9
HTTPS
certificate, obtaining 6-58
definition GL-3
log, viewing 6-45

I

images, device firmware 4-1
import command B-26
importing
device firmware 4-4
devices 6-28
templates 3-135
installing software updates 6-52, B-28, B-29, B-60
interface command B-30
inventory
client associations inventory 6-24
history 6-27
immediate inventory
of all devices 6-26

Downloaded from www.Manualslib.com manuals search engine

of selected devices 6-25
performance attributes polling interval, setting 6-73
performance inventory 6-24
polling interval, setting 6-73
resetting the polling interval 6-73
scheduled 6-24
IP addresses
displaying 6-18, B-25
in UI, display of 1-5
mapping to hostnames B-26
translating to hostnames B-36
IP chains, displaying B-60
ip domain-name command B-31
ip name-server command B-32
IP port filters, configuring 3-23
IP protocol filters, configuring 3-18

J

jobs, configuration
copying 3-148
creating 3-144
deleting 3-148
editing 3-148
filtering 3-147
managing 3-137
naming guidelines A-1
troubleshooting 8-3
undoing 3-149
viewing status 3-144
jobs, email 5-68
jobs, firmware
creating 4-10, 4-18
deleting 4-22
editing 4-10, 4-21
filtering 4-21
job run details 4-22
managing 4-9
naming guidelines A-1
troubleshooting 8-8
viewing 4-19
jobs log, displaying 6-46

L

LEAP server
adding 6-33
definition GL-4
EAP authentication report, displaying 5-30
setting response time 2-7
setting up 6-16
summary report, displaying 5-49
Links subtab 6-81
listbackup command B-33
local
admin access, configuring 3-92
AP/client security, configuring 3-94
logging in

Downloaded from www.Manualslib.com manuals search engine

splash screen, adding a message 6-69
to WLSE 1-7
troubleshooting 8-14
logging out
CLI command for B-10
from the WLSE 1-6
logs, displaying
bootlog B-51
collector log B-53
daemon manager log 6-45, B-56
daemons log 6-45, B-55
email logs B-62
install logs B-60
repository access log B-63
security log B-64
syslog B-67
system log 6-69
Tomcat log 6-45, B-69
View Log File option 6-45
Web access log 6-45, B-57
Web error log 6-45, B-58
Web SSL access log B-59

M

MAC address, displaying B-13
mailcntrl clear command B-35
mailcntrl list command B-35
mail command B-34
mailroute command B-36
mail server, specifying 6-71
maintenance image, CLI commands for B-75
Manage/Unmanage option 6-2
Managed Devices option 6-2
Manage Roles option 6-75
Manage Users option 6-77

N

name servers, specifying 6-71, B-32
naming guidelines A-1
neighbors, displaying B-52
network
connectivity testing 6-72
setting up 6-12
network interfaces
configuring B-30
displaying B-13
IP chains, displaying B-60
notification settings, faults 2-20
nslookup
definition GL-4
nslookup CLI command B-36
NSlookup tool 6-72
NTP (Network Time Protocol)
configuring 6-70, B-37
definition GL-4
ntp server command B-37

Downloaded from www.Manualslib.com manuals search engine

P

parameters, system 6-73
passwords
  changing your password 6-80
  EAP-MD5 server 6-36
  HTTP 6-9
  LEAP server 6-33
  RADIUS server 6-35
  WLSE users 6-77
performance
  inventory 6-24
  parameters for data collection 6-73
performance graph, displaying for access points and bridges 5-60
performance table, displaying for access points and bridges 5-61
per VLAN client (group) report, displaying 5-20
ping
  CLI command B-10
  definition GL-5
  Ping tool 6-72
policy
  AP report, displaying 5-36
  group report, displaying 5-21
  groups, configuring 3-28
  setting for profiles 2-7
port
  assignments, configuring 3-47
  filtering, configuring B-24
processes, displaying 6-66, B-13, B-62
profiles, managing 2-7
  assigning 2-10
  copying 2-8
  creating 2-8
  deleting 2-10
  editing 2-9
  renaming 2-9
  viewing devices for 2-11

Q

quality of service (QoS)
  configuring 3-36
  report, displaying 5-38

R

radio
  11a, configuring 3-73
    advanced 3-81
    data encryption 3-89
    filters 3-75
    hardware 3-76
    identification 3-73
    searched channels 3-88
  11b, configuring 3-56
    advanced 3-66

Downloaded from www.Manualslib.com manuals search engine

filters 3-59
hardware 3-60
identification 3-56
searched channels 3-71
RADIUS
authentication module 6-57
definition GL-5
RADIUS server
adding 6-35
EAP authentication report, displaying 5-30
setting response time 2-7
setting up 6-16
summary report, displaying 5-49
reader comment form, submitting electronically xvi
rebooting, WLSE 6-47, B-39
reload command
maintenance image command B-76
Privilege Level 15 command B-39
reports
current, displaying 5-11
device center, using 5-1
emailing 5-66
exporting 5-66
parameters for 6-73
scheduling email 5-68
trends, displaying 5-50
troubleshooting 8-9
wireless client, displaying 5-6
repository
browsing 6-53
creating
local 6-50, B-40
remote 6-51, B-27
definition GL-5
listing images and updates B-28, B-43
local
deleting software from B-42
status B-44
transferring software to B-41
status, displaying B-63
restarting (rebooting) WLSE 6-47
bootlog, displaying B-51
Restart option 6-47
restore command B-45
restoring data from backups 6-61, B-45
reverse DNS lookup 6-18
roles
creating and modifying 6-75
deleting 6-75
naming guidelines A-1
predefined 6-75
route command B-46
router
AP and Bridge connected to, displaying 5-48
fault thresholds, setting 2-7
setting up 6-15
summary report, displaying 5-47
system-defined group for 6-37

Downloaded from www.Manualslib.com manuals search engine

routes
adding B-46
displaying B-15, B-64
routing, configuring 3-111
Run Discovery Now option 6-22

S

scheduling
configuration jobs 3-138
discovery 6-20
email 5-68
firmware jobs 4-18
security
authentication
enabling B-17
modules 6-56
configuring 3-92
local admin access 3-92
local AP/client 3-94
server-based 3-97
HTTPS 6-58
last 10 logged in users, viewing 6-60
log, displaying B-64
SSH 6-59
SSL 6-58
Telnet, enabling or disabling 6-59
seed
adding seeds 6-20
definition GL-6
server
response time graph, displaying 5-65
security, configuring 3-97
setting response time 2-7
summary report, displaying 5-49
services, configuring
accounting 3-119
CDP 3-112
console/Telnet 3-107
DNS 3-113
FTP 3-114
hot standby 3-109
HTTP 3-116
routing 3-111
SNMP 3-117
SNTP 3-118
start-up 3-103
services, managing B-46
services command B-46
service sets, configuring 3-38
short term trending inventory truncation interval, setting 6-73
show auth-cli command B-49
show auth-http command B-49
show backupconfig command B-50
show bootlog command B-51
show cdp-neighbor B-52
show cdp-run command B-52
show clock command B-11

Downloaded from www.Manualslib.com manuals search engine

show config command B-54
show domain-name command B-12
show import command B-59
show interfaces command B-13
show process command B-13
show route command B-64
show ssh-version command B-66
show syslog command B-67
show tech command B-68
show version command B-14
shutdown command B-70
SMTP
  definition GL-6
  server, specifying 6-71, B-36
SNMP
  agent, configuring B-71
  agent log, displaying 6-46
  community strings
    guidelines for 6-9
    specifying 6-7
  configuration, displaying B-66
  definition GL-6
  reachability, testing 6-72
  template 3-117
  trap notification
    MIB 2-21
    setting 2-21
snmp-server command B-71
SNTP, configuring 3-118
software, on devices
  firmware, managing 4-1
  groups for 6-37
software, on WLSE
  browsing the repository 6-53
  deleting images from local repository B-42
  installation log, displaying 6-46, B-60
  listing images B-43
  local repository, creating 6-50, B-27, B-40
  maintenance image B-75
  managing 6-47
  overview 6-47
  remote repository, creating 6-51, B-27
  repository access log B-63
  status, viewing 6-48, B-44, B-63
  transferring images from remote to local repository B-41
  updates
    history, viewing 6-54, B-28
    images, viewing B-28
    installing 6-52, B-29
    listing B-43
    transferring to WLSE B-41
  version, viewing 1-4, B-14
splash screen, adding a message 6-69
SSH
  definition GL-6
  enabling 6-59, B-72
  type, displaying B-66
ssh-version command B-72

Downloaded from www.Manualslib.com manuals search engine

SSID
definition GL-6
report, displaying 5-40
system-defined groups for 6-37
SSL
certificate, obtaining 6-58
definition GL-6
log, displaying 6-46, B-59
managing 6-58
startup configuration
assigning 3-151
creating a template for 3-153
start-up settings, configuring 3-103
subnet, system-defined group for 6-37
summary report
access point 5-24
router 5-47
server 5-49
switch 5-45
switch
AP and bridge connected to report, displaying 5-46
fault thresholds, setting 2-7
setting up 6-15
summary report, displaying 5-45
system-defined group for 6-37
syntax of commands, checking B-2, B-3
syslog
displaying B-67
notification, setting 2-22
sysName, display of 6-18
system
configuration
displaying B-54
erasing B-23
gateway, specifying B-30
hostname, changing B-25
interfaces, configuring B-30
rebooting 6-47, B-39
shutdown B-70
SNMP, configuration B-71
SNMP configuration B-66
storage usage, displaying B-22
system log, using 6-69
system parameters, setting 6-73

T

TAC (Technical Assistance Center)
information for, displaying B-68
obtaining support from xvii
how the Escalation Center works xviii
priority levels, understanding xvii
telephone numbers xviii
website xviii
TACACS+
authentication module 6-56
definition GL-7
TCP Port Scan tool 6-72

Downloaded from www.Manualslib.com manuals search engine

Technical Assistance Center (see TAC) xvii
technical support xvi
through Cisco.com xvii
through TAC xvii
telephone numbers for TAC (see technical support) xviii
Telnet
disabling B-73
enabling 6-59, B-73
SSH 6-59
status, displaying B-68
Telnet/console services, configuring 3-107
telnetenable command B-73
templates
automatic configurations 3-151
copying 3-133
creating 3-132
deleting 3-134
editing 3-134
exporting 3-137
importing 3-135
troubleshooting 8-3
using 3-1
TFTP
definition GL-7
setting up on access points 6-14
threshold
definition GL-7
specifying fault threshold 2-7
time
browser time, setting 6-69
display on WLSE 1-5
synchronizing to an NTP server 6-70, B-37
system time 1-5
UTC
definition GL-7
displaying B-11
display of 1-5
setting B-11
timeout period 1-2
tomcat log, displaying 6-46, B-69
top n number of associations report, displaying 5-54
top n percentage errors report, displaying 5-55
traceroute
command B-15
definition GL-7
Traceroute tool 6-72
transmission statistics
displaying Ethernet for AP and bridge 5-58
displaying RF for AP and bridge 5-56
traps
MIB to define 2-21
setting for notification 2-21
trends, displaying 5-50
AP and bridge Ethernet transmission statistics 5-58
AP and bridge performance graph 5-60
AP and bridge performance table 5-61
AP and bridge RF transmission statistics 5-56

Downloaded from www.Manualslib.com manuals search engine

group performance report, Ethernet utilization 5-53

group performance report, RF utilization 5-51

server response time graph 5-65

top n busiest clients 5-62

top n client error rate 5-64

top n number of associations report 5-54

top n percentage errors report 5-55

troubleshooting 8-1

configuration 8-3

device management 8-11

discovery 8-11

firmware 8-8

reports 8-9

users 8-14

typographical conventions

in command descriptions B-9

used in this document xiii

U

undoing a job 3-149

unmanaged devices 6-3

user-defined

groups 6-39

roles 6-75

username command B-74

users

CLI access 6-77

creating 6-77, B-74

deleting 6-80, B-74

last 10 logged in users. viewing 6-60

modifying 6-77

naming guidelines A-1

password, changing 6-80

removing 6-77

roles

assigning to users 6-77

managing 6-75

troubleshooting 8-14

UTC

definition GL-7

displaying B-11

on WLSE 1-5

setting B-21

V

VLAN

AP report, displaying 5-42

configuring 3-31

group report, displaying 5-18

per client report (group), displaying 5-20

per client report (individual), displaying 5-20

system-defined groups for 6-38

Downloaded from www.Manualslib.com manuals search engine

W

Web access log, displaying **6-46, B-57**
Web error log, displaying **6-46, B-58**
Web SSL log, displaying **B-59**
WEP keys, definition **GL-8**
wireless client polling, setting **6-73**
wireless client reports, displaying **5-6**
  client detail **5-6**
  client historical association **5-9**
  client statistics **5-8**
World Wide Web
  contacting TAC via **xviii**
  obtaining Cisco documentation via **xv**

Downloaded from www.Manualslib.com manuals search engine